# Universidad Nacional de Loja

## Facultad de la Energía, las Industrias y los Recursos Naturales No Renovables

### Maestría en Telecomunicaciones

# Análisis de la influencia de los ciberataques para la generación de políticas públicas en el Ecuador en el ámbito de la gobernanza del Internet.

**Trabajo de Titulación previo a la obtención del título de Magister en Telecomunicaciones.**


**AUTOR:**

Ing. Hugo Ernesto Acaro Gallegos

**DIRECTOR:**

Ing. John Tucker Yépez, Mg. Sc.


Loja – Ecuador

2023

## Certificación

Loja, 22 de mayo de 2023

Ing. John Jossimar Tucker Yépez Mg. Sc.
**DIRECTOR DE TRABAJO DE INVESTIGACIÓN**

**CERTIFICO:**

Que he revisado y orientado todo proceso de la elaboración del Trabajo de Titulación denominado: **Análisis de la influencia de los ciberataques para la generación de políticas públicas en el Ecuador en el ámbito de la gobernanza del Internet,** previo a la obtención del título de **Magíster en Telecomunicaciones**, de la autoría del estudiante **Hugo Ernesto Acaro Gallegos,** con **cedula de identidad N° 0921405692,** una vez que el trabajo cumple con todos los requisitos exigidos por la Universidad Nacional de Loja para el efecto, autorizo la presentación para la respectiva sustentación y defensa.


Firmado electrónicamente por:
JOHN JOSSIMAR
TUCKER YEPEZ

Ing. John Jossimar Tucker Yépez Mg. Sc.
**DIRECTOR DE TRABAJO DE INVESTIGACIÓN**

## Autoría

Yo, **Hugo Ernesto Acaro Gallegos,** declaro ser autor del Trabajo de Titulación y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos y acciones legales, por el contenido del mismo. Adicionalmente acepto y autorizo a la Universidad Nacional de Loja la publicación del Trabajo de Investigación en el Repositorio Digital Institucional – Biblioteca Virtual.

HUGO ERNESTO ACARO GALLEGOS

Firmado digitalmente por HUGO ERNESTO ACARO GALLEGOS
Fecha: 2023.05.29 15:18:28 -05'00'

**Firma:**

**Autor:** Hugo Ernesto Acaro Gallegos

**Cédula de Identidad:** 0921405692

**Fecha:** 29/05/2023

**Correo electrónico:** hugo.acaro@unl.edu.ec

**Teléfono:** 0998359467

**Carta de autorización por parte del autor, para consulta, reproducción parcial o total y/o publicación electrónica de texto completo, del Trabajo de Investigación.**

Yo, **Hugo Ernesto Acaro Gallegos,** declaro ser autor del Trabajo de Titulación denominado: **Análisis de la influencia de los ciberataques para la generación de políticas públicas en el Ecuador en el ámbito de la gobernanza del Internet,** como requisito para optar el título de **Magíster Telecomunicaciones**, autorizo al sistema Bibliotecario de la Universidad Nacional de Loja para que, con fines académicos muestre la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Institucional.

Los usuarios pueden consultar el contenido de este trabajo en el Repositorio Institucional, en las redes de información del país y del exterior con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia del trabajo de investigación que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los veintinueve días del mes de mayo de dos mil veintitrés.

HUGO ERNESTO ACARO GALLEGOS

Firmado digitalmente por HUGO ERNESTO ACARO GALLEGOS
Fecha: 2023.05.29 15:19:58 -05'00'

**Firma:**

**Autor:** Hugo Ernesto Acaro Gallegos

**Cédula:** 0921405692

**Dirección:** Daule

**Correo Electrónico:** hugo.acaro@unl.edu.ec

**Teléfono:** 0998359467

**DATOS COMPLEMENTARIOS:**

**DIRECTOR DE TRABAJO DE TITULACIÒN:** Ing. John Jossimar Tucker Yépez Mg. Sc.

## Dedicatoria

Dedico este trabajo de investigación a Dios por darme fuerzas para permitirme culminar esta etapa profesional. A mis padres por ser ese ejemplo de vida, constancia y sacrificio.

A mis hermanos, por ser ese apoyo en los momentos cuando más lo necesité.

A mi hija por su apoyo y comprensión en este proyecto y todos los demás proyectos que hemos vivido a lo largo de nuestras vidas.

A mis sobrinos que de una u otra manera me apoyaron en el proyecto.

***Hugo Ernesto Acaro Gallegos***

## Agradecimiento

Quiero agradecer a todos mis amigos que contribuyeron con este proceso y finalización de este proyecto en especial a Mónica que me ayudo cuando más lo necesité. A Nelson que supo compartir su experiencia en los inicios del proyecto.

A mi tutor Ing. John Tucker, por su paciencia, conocimientos y tiempo en el desarrollo del proyecto.

A mis compañeros de trabajo por todo su apoyo en todo este proceso.

A la Universidad Nacional de Loja, maestros y personas partícipes en el proceso. Por su aporte al país en la formación de profesionales.

***Hugo Ernesto Acaro Gallegos***

## Índice de Contenidos

**Índice de Tablas:**



**Índice de Figuras:**



**Índice de Anexos:**

## 1. Titulo

**Análisis de la influencia de los ciberataques para la generación de políticas públicas en el Ecuador en el ámbito de la gobernanza del Internet.**

## 2. Resumen

En el Ecuador según la Constitución de la República en el artículo 313 considera a las telecomunicaciones como parte del sector estratégico y como tal el estado tiene el derecho de administrar, regular, controlar y gestionar dicho sector. Así mismo se determinó que el acceso a la información es un derecho de los ciudadanos, sin embargo, el acceso a la información a través del Internet implica que se debe tener especial cuidado con todos los datos debido a la huella digital que dejamos en el ciberespacio. Esto es importante porque nuestros datos personales son un recurso muy valioso y debemos tomar todas las medidas de precaución para protegerla.

Dado a que la información hoy en día se encuentra expuesta y es relativamente fácil acceder a ella a través de Internet, se requieren varias herramientas legales para proteger a los ciudadanos y garantizar su seguridad frente a los ciberataques. Estos ataques evolucionan y mejoran constantemente junto con la tecnología, por lo que se ha determinado que los instrumentos legales deben adaptarse a estos cambios para mitigar significativamente los ataques y proteger a los ciudadanos. (F.E. Catota, M. G. Morgan y D. C. Sicker, 2018).

Para este fin, se examinarán las leyes escritas en nuestro país con respecto a la protección de los usuarios, como La ley Orgánica de Telecomunicaciones, La Ley Orgánica de Protección de Datos Personales y la Estrategia Nacional de Ciberseguridad del Ecuador. Esto permitirá generar políticas públicas en el ámbito de la gobernanza de Internet, lo que resultará en propuestas para mejorar la estrategia nacional de seguridad.

***Palabras Clave:*** *Ciberataques, gobernanza del Internet, ciberseguridad, políticas públicas, modelo multistakeholder, ciberespacio.*

## 2.1 Abstract

In Ecuador, according to the Constitution of the Republic in article 313 it considers telecommunications as part of the strategic sector and as such, the state has the right to administer, regulate, control, and manage said sector. Also, it was determinate that access to information is a right of citizens, however, access to information through the Internet implies that special care must be taken with all data due to the digital footprint that we leave in cyberspace. This is important because our personal data is a very valuable resource and we must take all precautionary measures to protect it.

Since information today is exposed and relatively easy to access through the Internet, various legal tools are required to protect citizens and ensure their security against cyber-attacks. These attacks are constantly evolving and improving along with technology, so it has been determined that legal instruments must adapt to these changes to significantly mitigate attacks and protect citizens.

For this purpose, laws written in our country regarding the protection of users will be examined, such as the Organic Law of Telecomunications, the Organic Law of Protection of Personal Data and the National Cyber security strategy of Ecuador. This will make it possible to generate public policies in the field of Internet governance, which will result in proposals to improve the national security strategy.



***Keywords:*** *Cyber-attacks, Internet governance, cybersecurity, public policies, multistake-holder model, cyberspace.*

## 3. Introducción

En la pandemia del Covid-19 se incrementó el uso del Internet, así como la virtualidad por el confinamiento. Es así como muchos de nosotros tuvimos que adaptarnos a la nueva realidad y hacer uso de herramientas como el Zoom, Anydesk, IPVPN y escritorios remotos que nos ayudan para trabajar desde casa. Esta nueva virtualidad hizo que a las empresas adaptaran la red interna de sus empleados para que tuvieran acceso desde sus hogares, lo que dio a conocer que muchas de las empresas no estaban preparadas para el trabajo remoto.

Anteriormente el Ecuador no era objeto de ciberataques, pero debido al confinamiento se incrementaron los ciberataques en especial a las empresas de infraestructura crítica (IC) que son objeto de constantes ataques, así como el sector bancario.

Debido a lo expuesto se analizará los ciberataques, así como la creación de las políticas públicas en el Ecuador para poder enfrentar y prevenir dichos ataques para que su daño tenga la menor afectación posible.

## 4. Teórico

El sector de las telecomunicaciones ha presentado un incremento importante tanto a nivel de avance tecnológico como en cantidad de usuarios. Según información de la ITU en el año 2022 en el Ecuador en comparación con el resto del mundo usaron Internet desde cualquier lugar en los últimos tres meses, el acceso puede ser a través de una red fija o móvil.

En base a lo expuesto se tiene los siguientes resultados:

El 51 % de usuarios del área rural accedieron al Internet en comparación con el 79 % de usuarios del área urbana. (Data explorer– ITU, 2022).

En niños de 14 años y adolescentes tuvieron acceso a Internet un 66%. En personas de 15 y 24 años tuvieron acceso a Internet un 87 % y en usuarios de 25 a 74 años tuvieron acceso a Internet el 70 %.

Estos porcentajes dan a conocer el uso continuo y necesario del ciberespacio. Sin embargo, el uso cada vez más frecuente del Internet nos obliga a tomar precauciones y exigir a nuestro ISP que nos informe de las medidas de seguridad que implementan para cuidar nuestra información a través de su red de acceso.

### 4.1 Influencia de los ciberataques

#### 4.1.1 Ciberespacio

El ciberespacio se define como un dominio global y dinámico. Es todo lo que utiliza Internet y cuyo propósito es crear, almacenar, intercambiar, compartir, modificar, extraer, usar y eliminar información. (C., 2022).

En el ciberespacio se realizan las actividades habituales en el diario vivir, como son las transacciones bancarias, compras en línea, actividades comerciales, redes sociales, correo electrónico, mensajería instantánea, entretenimiento, salud y educación. Por lo que se debe tener un cuidado y especial atención en la huella digital que dejamos en el espacio cibernético debido a que nuestra información personal es única y representa una nueva riqueza en la sociedad actual.

El ciberespacio al ser un entorno virtual permite el acceso de varias personas y estas se encuentran representadas o identificadas con un usuario que puede ser real o falso, dependiendo de las intenciones del individuo.

Con este entorno llamado ciberespacio donde no existe una frontera ni límite de tiempo se deben tener un nuevo tipo de protección que demanda nuevos conocimientos para protegerse de los ataques que puedan afectarnos con el fin de que nos afecte lo menos posible.

En el ciberespacio existe un nuevo entorno y este entorno tiene varias ventajas, pero también cuenta con sus desventajas y entre sus desventajas se encuentran los ciberataques. Este término se lo define a continuación:

### 4.2 Ciberataque

Los ciberataques son intentos no deseados de robar, exponer, alterar, inhabilitar o destruir información mediante el acceso no autorizado a los sistemas. (IBM, 2023).

Estos ataques son difíciles de detectar ya que el ciberatacante lo realiza de manera remota y anónima lo que le da una cierta ventaja o sensación de seguridad al realizar dicho ataque. Además, que puede utilizar nuestra información disponible del Internet para hacer un ataque direccionado y específico logrando tener una alta probabilidad de éxito.

Para prevenir estos ataques existe la recomendación UIT-T X.800, que da una visión general de los servicios de seguridad atribuidos a las siete capas del modelo de referencia de la interconexión de sistemas abiertos (OSI). (ITU, 2019).

En la recomendación RFC 2828 se define como un incidente de seguridad a un evento relevante para la seguridad, donde se desobedece o vulnera la política de seguridad poniendo en riesgo los recursos de una organización o sistema.

Existen varios tipos de ciberataques, entre los cuales tenemos los ataques pasivos, ataques activos, ataque intencional, ataque no intencional, ataques internos y ataques externos.

#### 4.2.1 Ataques pasivos

Un ataque pasivo sucede cuando el atacante, en este caso el ciberdelincuente se encarga de “escuchar” una comunicación no autorizada y la misma no se encuentra cifrada. (C., 2022).

#### 4.2.2 Ataques activos

Un ataque activo sucede cuando el atacante encuentra la vulnerabilidad, procede a capturar la información y realiza el cambio del contenido del mensaje. (A., 2021).

### 4.2.3 Ataque intencional

Los ataques intencionales son aquellos ataques que existen sin que sean premeditadas. (Universidad Complutense de Madrid, 2016).

### 4.2.4 Ataque no intencional

Los ataques no intencionados son los ataques donde no existe un objetivo deliberado de uso indebido. (Universidad Complutense de Madrid, 2016).

### 4.2.5 Ataques internos

Un ataque interno es un ataque que es iniciado dentro del perímetro de seguridad. (Bertolín, J. A., 2020).

### 4.2.6 Ataques externos

Un ataque externo es un ataque que es iniciado desde fuera del perímetro de seguridad, por un usuario no autorizado o ilegítimo.

Todos estos tipos de ataque afectan el desarrollo, evolución y uso del ciberespacio. (J.E. Alvarado, 2020).

Una vez que hemos revisado los tipos de ataques que afectan el ciberespacio, analizaremos la influencia de los organismos internacionales y cuáles son sus implicaciones en la ciberseguridad de sus países miembros.

## 4.3 Influencia de los organismos Internacionales

Los Estados tienen un rol muy importante a nivel de ciberseguridad. Estos estados deben regular, proponer y gestionar mecanismos para garantizar a sus usuarios el uso seguro del ciberespacio. Esto garantiza el derecho y uso a la información. A nivel de ciberseguridad siempre se trata de ubicar a los países en términos de ciberseguridad, aunque es difícil proporcionar una respuesta exacta, en especial en un campo donde la tecnología evoluciona de forma exponencial y los sistemas de información pueden ser atacados en cualquier momento, se puede presenciar que los países poco a poco están asumiendo el compromiso en materia de ciberseguridad, esto debido a la importancia que tiene la información para sus usuarios.

Este compromiso deja en claro los deberes, derechos y obligaciones que tienen los actores involucrados (proveedores y usuarios) dando paso a la creación de mecanismos necesarios para la

protección de la información. La revisión y seguimiento al compromiso adquirido a nivel de ciberseguridad es complicado ya que dependen de varios factores. Sin embargo, están surgiendo iniciativas que pretenden dar características que debe tener un país para sirva de ejemplo y poder mejorar a nivel de ciberseguridad.

Estas iniciativas están surgiendo desde varios puntos, desde lo global como es el caso de las Naciones Unidas a través de la UIT, la Organización de Estados Americanos o la Unión de Naciones Suramericanas, hasta de forma local o a nivel de estado.

### 4.3.1 Naciones Unidas (ONU)

La Organización de las Naciones Unidas (ONU) nació una vez finalizada la segunda guerra mundial, cuando representantes de 50 países se reunieron en San Francisco (EEUU) en la conferencia de las Naciones Unidas sobre Organización Internacional, que se efectuó del 25 de abril al 26 de junio de 1945 luego de 2 meses de conferencia. Esto con el fin de evitar otra guerra y ayudar a los países a mantener la paz y seguridad internacional. Para esto y con el objetivo de ayudar a los demás países la ONU tiene un organismo especializado que se encarga de las tecnologías de información y comunicación TIC y es la UIT. (CEPAL, 2023).

La UIT es un organismo fundado en 1865 y su función es la de facilitar la conectividad internacional de las redes de comunicación, el espectro de frecuencias radioeléctricas y las órbitas satelitales. También elaboran normas técnicas para la interconexión de redes y tecnologías en especial para aquellos países menos atendidos en el mundo. (UIT, 2022).

La UIT publicó el 9 de diciembre de 2014, en el Telecom World 2014 (Doha), el Global Cybersecurity Index, que es un trabajo de investigación en donde se elaboró un documento y se evaluó el compromiso de las naciones con la ciberseguridad. Se pidió la participación voluntaria de los países donde se solicitó llenar un formulario en el cual se planteaba cinco aspectos y estas fueron:

- Medidas legales.
- Medidas técnicas.
- Medidas orgánicas.
- Capacitación.

- Cooperación.

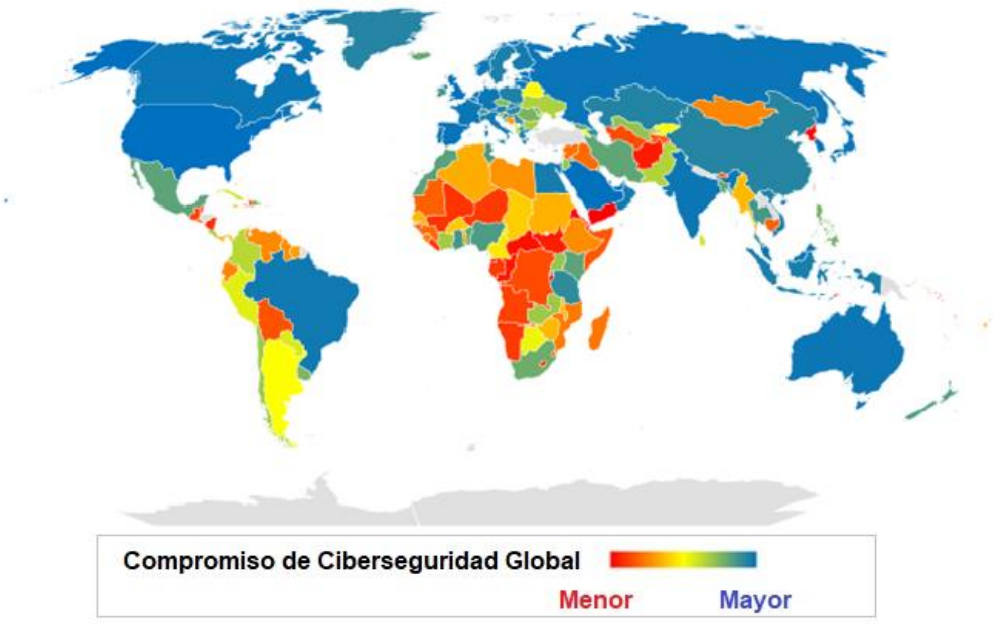
Desde la edición del año 2014, los países fueron ingresando a la Unión Internacional de Telecomunicaciones UIT, en ese entonces participaron 104 países y los países que no enviaron la información solicitada fueron 194. (Moran, D.R., 2015).

En su primera edición, el primer lugar lo ocupó Estados Unidos, seguido por Canadá. (UIT, 2022).

En Iberoamérica el nivel de compromiso tomó valores intermedios salvo casos puntuales. Fueron casos positivos como de Brasil, así como negativos en el caso de Honduras, igualando o incluso superando los valores medios registrados en el continente asiático, aunque por debajo de los países europeos. El continente africano y oriente próximo tuvieron las menores calificaciones de la lista de países, como se observa en el mapa de compromiso.

**Figura 1**

Grado de compromiso global




*Fuente:* Página web ITU

En Sudamérica los países que cuentan con estrategia de ciberseguridad son Perú, Brasil, Chile, Colombia, Ecuador, y Trinidad y Tobago, según información del Índice Mundial de Ciberseguridad del año 2020.

Actualmente se tiene 194 países miembros que enviaron la información a la UIT según información del año 2020. (ITU, 2021).

### 4.3.2 OEA

La OEA (Organización de Estados Americanos) es el organismo regional más antiguo del mundo. Su origen se remonta a la Primera Conferencia Internacional Americana, realizada en Washington, DC de octubre de 1889 hasta abril de 1890. La OEA fue creada en 1948 en Bogotá, Colombia y su objetivo es según lo estipula el artículo 1 de la Carta lograr "un orden de paz y de justicia, fomentar su solidaridad, robustecer su colaboración y defender su soberanía, su integridad territorial y su independencia". (OEA, 2023).

La OEA elaboró en 2004 la Estrategia de Ciberseguridad basada en tres pilares: CICTE, CITEL y REJMA, constituidos por grupos de expertos. A continuación, se informa los tres pilares establecidos por la OEA:

- CICTE (Comité Interamericano contra el Terrorismo): persigue la formación de una red de vigilancia, alerta y aviso interamericana esto con el fin de combatir el terrorismo. Así puede avisar de forma inmediata la intrusión y poder actuar de manera rápida y solucionar las amenazas a la seguridad informática.
- CITEL (Comisión Interamericana de Telecomunicaciones): Se encarga de promover el continuo desarrollo de las TIC. Además de organizar y evaluar reuniones técnicas, de operación, construcción, planificación, normalización, asistencia técnica, mantenimiento y demás asuntos relacionados con las telecomunicaciones en las Américas.
- REMJA (Reuniones de Ministros de Justicia u otros Ministros, Fiscales y Procuradores Generales de las Américas: asegura el punto de encuentro de las autoridades judiciales de las Américas para el intercambio de información y coordinación de políticas públicas. (Moran, D.R., 2015).

La OEA también publica de forma periódica en materia de ciberseguridad los informes donde se incluyen lo más importante en la región de Latinoamérica y el Caribe, así como una evolución en la implementación de medidas de seguridad en la red de sus países miembros.

## 4.4 Generación de políticas públicas

### 4.4.1 Políticas públicas

La política pública es un instrumento de transformación de la sociedad que actúa sobre los comportamientos de las personas. Estas políticas públicas las crea y genera el gobierno por medio de una administración pública. Estas políticas públicas pueden ser acciones o inacciones que se crean o gestionan para solucionar un problema. (Las políticas públicas y la gestión pública: un análisis desde la teoría y la práctica, 2019).

En el desarrollo de las Telecomunicaciones y las Tecnologías de Información y Comunicaciones (TIC), se ha presenciado un gran incremento en el Internet y ciberespacio en especial por el confinamiento debido a la pandemia del COVID19 que aceleró la virtualidad y el trabajo remoto provocando que nos adaptemos a una nueva realidad. Esto ha provocado que los gobiernos de América Latina y el Caribe, prioricen las políticas públicas, analicen modificaciones y actualizaciones de acuerdo a la nueva realidad.

### 4.4.2 Generación de políticas públicas en el Ecuador

En el sector de telecomunicaciones y de la sociedad de la información, siempre se busca que exista un beneficio entre los encargados de brindar los servicios de telecomunicaciones (ISP) y los abonados, además de dar prioridad a los abonados al acceso y derecho a la información. Esto fomentará la libre competencia, así como la implementación de tarifas orientadas al usuario, garantizando un servicio de calidad de acuerdo al servicio y la economía según el mercado actual. (Comisión Europea, 2014).

Para garantizar el acceso, uso y seguridad en el ciberespacio, el estado ecuatoriano ha creado políticas públicas que nos ayudan a gestionar y afrontar de mejor forma los ciberataques y estas son:

- Ley Orgánica de Telecomunicaciones.
- Ley Orgánica de Protección de Datos Personales.
- Estrategia Nacional de Ciberseguridad del Ecuador.

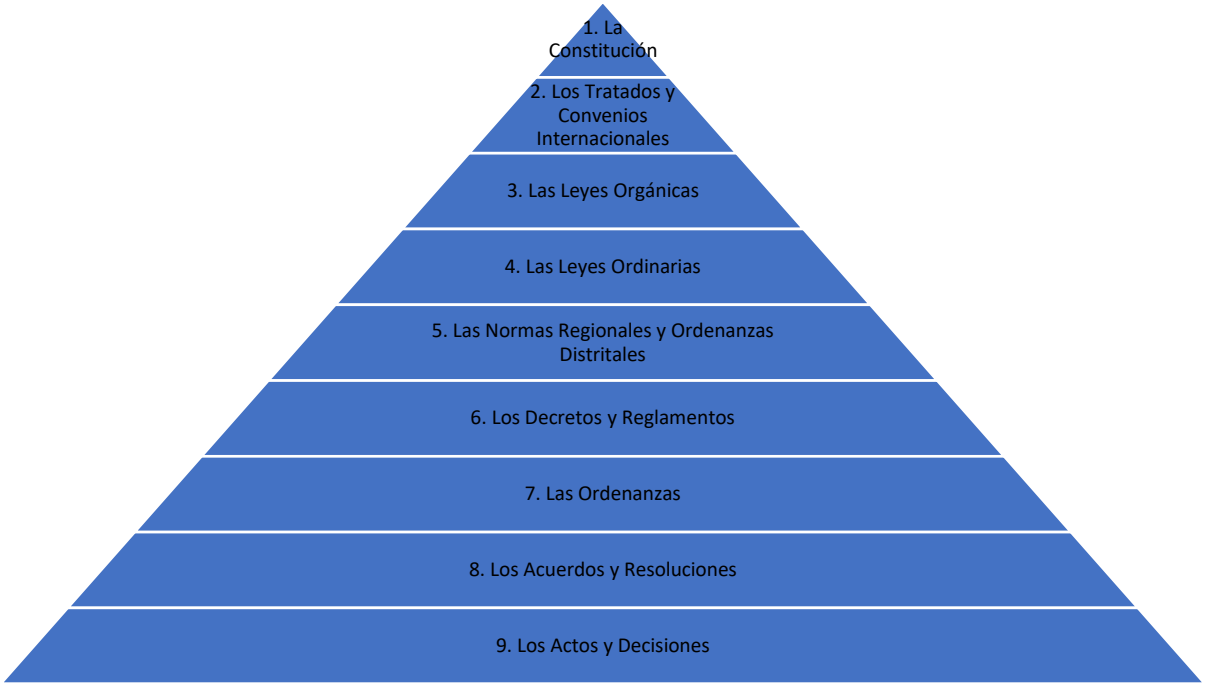
Bajo este principio se debe formular un marco regulatorio que esté acorde a la legislación vigente y a su vez debe estar alineado con la conocida pirámide de Kelsen.

Cuando se mencionan las políticas públicas es necesario mencionar la pirámide de Kelsen por lo que se lo explica a continuación.

La pirámide de Kelsen menciona el orden de relación de las normas según su jerarquía, quedando organizado de la siguiente manera:

**Figura 2**

Pirámide de Kelsen según normativa ecuatoriana




*Fuente:* Constitución del Ecuador

Se debe tener en cuenta que la pirámide de Kelsen representa de forma gráfica el sistema jurídico en Ecuador según el artículo 425 de la Constitución de la República del Ecuador que prescribe: “El orden jerárquico de aplicación de las normas será el siguiente: La constitución, los tratados y convenios internacionales; las leyes orgánicas; las leyes ordinarias; las normas regionales; y los demás actos y decisiones del poder público.

En caso de conflicto entre normas de distinta jerarquía, la corte Constitucional, las juezas y jueces, autoridades administrativas y servidoras y servidores públicos, lo resolverán mediante la aplicación de la norma jerárquica superior’’.

Después de analizar el tema de ciberseguridad y para contrarrestar las amenazas en el ciberespacio, el Ministerio de Telecomunicaciones y de la Sociedad de la Información al mando de la Ministra Abg. Vianna Maino decidió crear como mecanismo de protección La Estrategia Nacional de Ciberseguridad. Esta estrategia fue realizada con el apoyo del Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo, de la Organización de los Estados Americanos (CICTE/OEA) Y AL Proyecto de Resiliencia Cibernética para el Desarrollo, de la Unión Europea (CYBER4DEV). (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2022).

Con este apoyo el Ecuador da un paso muy importante en materia de ciberseguridad debido que este documento tuvo la participación de 170 actores de la sociedad civil, académicos, expertos en ciberseguridad, funciones del estado, sector privado y todas las instituciones que conforman el Comité Nacional de Ciberseguridad.

Se debe tener tomar en consideración que el Comité Nacional de Ciberseguridad fue creado en el gobierno del Presidente Guillermo Lasso y este se encuentra conformado por el Ministerio de Telecomunicaciones y de la sociedad de la Información, Defensa Nacional, Gobierno, Interior, Relaciones exteriores y Movilidad Humana, el Centro de Inteligencia Estratégica y la secretaria General de la Administración Pública de la Presidencia.

Esta estrategia tendrá como aplicación los próximos tres años (2022 – 2025) y sus pilares se basan en 6 ejes de acción prioritarios para el país que son:

- Gobernanza y Coordinación Nacional.
- Resiliencia cibernética.
- Prevención y combate a la ciberdelincuencia.
- Ciberdefensa.
- Habilidades y Capacidades de Ciberseguridad.
- Cooperación Internacional.

Con esta estrategia nacional de Ciberseguridad el país acepta el desafío y la oportunidad de crecimiento a nivel de Ciberseguridad, con esto el país desde una perspectiva jurídica adopta medidas para ratificar y aplicar al convenio de Budapest sobre la Ciberdelincuencia, teniendo como resultado que el país sea invitado el 30 de marzo del año 2022 a adherirse al tratado. Con

esta invitación al convenio de Budapest el país tendrá la capacidad de combatir la ciberdelincuencia transfronteriza dando un paso muy importante en la lucha contra la ciberdelincuencia. (Tapuia, 2005).

### 4.4.3 Políticas públicas en el ámbito de redes y el ciberespacio

La seguridad en el ciberespacio representa un punto muy importante en las políticas de un Estado. Además, que el uso del Internet y el ciberespacio para las actividades sean del estado, así como de la sociedad en general nos hacen cada vez más dependientes. Esto hace más fácil el ataque del ciberdelincuente, debido a que los ataques no tienen un límite de tiempo ni frontera física y las amenazas a la seguridad de un estado afectan tanto al país como a sus ciudadanos.

Por tanto, la seguridad cibernética se ha convertido en un aspecto muy importante para la seguridad nacional, pero el estado ecuatoriano al ser un país en vías de desarrollo presenta vulnerabilidades. Se puede apreciar cada vez que las ciberamenazas y los ciberdelitos son cada vez más complejos, además de ser más específicos y detallados llegando a tal punto de convertirse en ciberespionaje a nivel militar, empresarial y político. Por lo que el estado busca cada vez optimizar los recursos económicos, humanos y técnicos que dispone al momento para hacer frente a estas amenazas en la actualidad.

El Ministerio Nacional de Defensa, señala al ciberespacio como prioritario para la seguridad del Estado y sus ciudadanos haciéndolo parte del territorio nacional. Por lo que cuando exista un ataque al territorio nacional, el estado debe proteger también el ciberespacio.

Debido a esto la estrategia planificada por el gobierno garantiza la continuidad y complementariedad de las iniciativas existentes. (L.M. 2021). Estas se informan a continuación:

- **El Plan Nacional de Desarrollo (2021 – 2025)** establece el fortalecimiento de la conectividad y acceso a las tecnologías de información y las comunicaciones (TIC), el aumento de la cobertura y el acceso a los servicios móviles de alta velocidad y la mejora de la posición internacional del Ecuador.
- **La Política Nacional de Ciberseguridad**, cuyo objetivo es construir y fortalecer las capacidades que permitan garantizar el ejercicio de los derechos y libertades de la población, así como la protección de los bienes jurídicos del estado en el ciberespacio.

- **El Plan Específico de Seguridad Pública y Ciudadana (2019 – 2030)** que fija objetivos para combatir los delitos transnacionales, entre ellos el delito cibernético. Además, que propone dotar de equipamiento a una unidad de Ciberinteligencia en la Policía Nacional.
- **El Plan Específico de Relaciones Exteriores y Movilidad Humana (2019 – 2030)** destaca el impacto de varias amenazas en la economía, la seguridad integral y la información.
- **El Plan Específico de Defensa (2019 – 2030)** prevé la participación activa del Ecuador en el control efectivo del territorio nacional (aire, tierra, mar y ciberespacio), promoviendo el desarrollo de políticas y estrategias relativas al ciberespacio y Ciberdefensa.
- **El Plan Estratégico de Defensa Institucional (2017 – 2021)** encomienda a las Fuerzas Armadas a evaluar constantemente los escenarios de amenazas, riesgos por lo que debe actualizar las capacidades de defensa.

## 4.5 Gobernanza del Internet

### 4.5.1 Historia

#### 4.5.1.1Cumbre Mundial de la Sociedad de la Información (WSIS)

El debate sobre la gobernanza de Internet fue promovido desde la Cumbre Mundial de la Sociedad de la Información (WSIS) y esta fue una iniciativa de las Naciones Unidas y la Unión Internacional de Telecomunicaciones. Esta cumbre que fue realizada en dos fases (Ginebra 2003 y Túnez 2005) empezó como un primer impulso para dar respuesta a varias preguntas surgidas en torno al creciente fenómeno de la gobernanza de Internet y tratar, además temas importantes a lo que se refiere a la Sociedad de la Información.

En la primera fase realizada en Ginebra en diciembre de 2003, uno de los temas centrales fue el análisis de las diferentes estrategias de financiación global de las TIC destinadas a reducir progresivamente la brecha digital entre las demás regiones. Junto con los mecanismos de financiación, el debate se centró en la gobernanza de Internet, en donde los gobiernos reconocieron el papel muy importante del Internet como el elemento que sustenta o apoya a la Sociedad de la Información y Conocimiento, debido a esto se mostró una preocupación a las opiniones que surgían en la gestión de sus recursos, así como del papel que cumplen la regulación y las políticas públicas enfocadas a Internet.

En base a esto, decidieron crear un grupo de trabajo de gobernanza en el seno de la conferencia (WGIG), que elaboró un informe que se presentó en la siguiente fase de la WSIS que se realizó en Túnez, con los siguientes objetivos generales:

- Elaborar una definición sobre el concepto de gobernanza de Internet que pudiera ser comúnmente aceptada.
- Identificar los aspectos más relevantes en materia de regulación, normativas y políticas públicas relacionadas con el fenómeno de la gobernanza de Internet.
- Avanzar en la identificación del papel que desempeñan en el contexto de la gobernanza los gobiernos nacionales y supranacionales, las organizaciones intergubernamentales e internacionales, el sector privado y la sociedad civil tanto en países en desarrollo como en países desarrollados.

En este primer encuentro, las visiones de lo que debería ser la gobernanza de la infraestructura técnica de la red, quedaron entre dos posiciones completamente opuestas: por un lado, los partidarios de ICANN (favorables a mantener la situación que prevalece desde el nacimiento de Internet) insistían en que cualquier cambio en el sistema era realizable dentro de la estructura existente. Por otro lado, quedaron todos aquellos que independientemente de su pertenencia al WGIG, eran partidarios de una transferencia progresiva de funciones desde ICANN hacia la Unión Internacional de las Telecomunicaciones.

Después de la conformación del grupo, se realizó la segunda fase, y fue realizada en Túnez en el mes de noviembre del año 2005, esta segunda fase sirvió de foro para presentar y valorar los resultados obtenidos. Cabe destacar en primer lugar la definición del concepto de gobernanza como primer resultado obtenido por el grupo (WGIG, 2005) que se definió de la siguiente manera:

«La gobernanza de Internet es el desarrollo y la aplicación por los gobiernos, el sector privado, y la sociedad civil, en las funciones que les competen respectivamente, de principios, normas, reglas, procedimientos de adopción de decisiones y programas comunes que configuran la evolución y utilización de Internet.».

En otro aspecto, la principal conclusión del trabajo desarrollado por el WGIG fue que la gobernanza de Internet no se enfoca exclusivamente a cuestiones sólo técnicas como son la gestión de los recursos críticos de Internet sino que implica también un enfoque más amplio donde son importantes los puntos como la reducción de la brecha digital y desarrollo de la sociedad del

conocimiento, el respeto a la libertad de información y expresión, la ciberseguridad, la preservación de la identidad cultural y del idioma propio.

Se reconoció además la necesidad de que cada estado diseñe sus propias políticas públicas haciendo énfasis a los criterios de índole nacional y territorial en el tema de cultura, idioma y respeto a las libertades de cada persona, siempre en relación con los convenios y acuerdos internacionales. (Tapuia. 2005).

En conclusión, se acordó que todos los gobiernos debían tener un papel importante en la gobernanza de Internet para garantizar la estabilidad, seguridad, continuidad de Internet y el ciberespacio, debido a esto se invitó a todos los agentes involucrados en la gobernanza a enfocarse en una misma dirección basada en el diálogo, así como la colaboración con la comunidad académica y científica especializada.

#### 4.5.1.2 Foro de la gobernanza de Internet (IGF)

Uno de los acuerdos en la segunda fase de la Cumbre fue el de fomentar la internacionalización de la gobernanza de Internet y el desarrollo de la cooperación intergubernamental. Como resultado de estos acuerdos se creó el IGF (Internet Governance Fórum), un espacio abierto y descentralizado para el debate sobre políticas que ayuden a la sostenibilidad y solidez del Internet, el sector privado, colectivos académicos y de investigación, y la sociedad civil.

El IGF fue considerado como la continuación de los trabajos WGIG en línea con los acuerdos alcanzados durante la WSIS, y se constituye como un espacio multilateral, democrático y transparente para el diálogo político, cuya misión incluye, entre otros, la facilitación del diálogo sobre los diferentes aspectos del gobierno de Internet, que en el futuro pueden influir en su desarrollo.

La primera reunión celebrada en Ginebra en febrero de 2006, acogió a representantes de todos los colectivos involucrados. En este encuentro se acordaron las líneas de desarrollo del IGF, se plantearon cuestiones relativas a las actividades, prioridades y funcionamiento del Foro; es decir, se llegó a un entendimiento común sobre la naturaleza y carácter del IGF. También se estableció la necesidad que un grupo compuesto por las distintas partes tenga el encargo de identificar los temas del ámbito de las políticas públicas que examinará en cada una de las posteriores reuniones.

Concluida la reunión, el primer encuentro oficial del Foro se celebró en Atenas del 30 de octubre al 2 de noviembre del año 2006. Durante la reunión, el debate político y las contribuciones de los diferentes colectivos se desarrollaron en torno a cuatro grandes temas que son:

- Apertura.
- Seguridad.
- Diversidad.
- Acceso.

Con este foro se dio inicio a la importancia de la gobernanza del Internet, trayendo consigo la continuidad y necesidad de los temas relacionados al Internet y su diálogo político entre los países miembros. (Fundación Telefónica, 2023).

### 4.5.2 Gobernanza del Internet y su alcance

Según la UNESCO, la gobernanza de Internet es el desarrollo y la aplicación complementaria de los gobiernos, el sector privado, la sociedad civil y la comunidad técnica en sus respectivas funciones, de los principios, normas, reglas, procedimientos de tomas de decisiones y actividades compartidas que dan forma a la evolución y uso de Internet. Para la UNESCO la gobernanza de Internet es un tema fundamental debido al potencial que tiene internet para fomentar el desarrollo humano sostenible y la construcción de sociedades del conocimiento inclusivas, a fin de mejorar la libre circulación de información e ideas en el mundo entero. (UNESCO, 2023).

Para empezar a entender el concepto de gobernanza es necesario comprender y diferenciar correctamente los siguientes términos:

- Gobierno: Acción y efecto de gobernar o gobernarse.
- Gobernabilidad: Modo o estilo de gobierno caracterizado por el grado de cooperación e interacción entre gobierno y actores no estatales.
- Gobernación: Ejercicio del gobierno.
- Gobernanza: Arte o manera de gobernar que tiene como objetivo el desarrollo económico, social e institucional duradero, promoviendo un sano equilibrio entre el Estado, la sociedad civil y el mercado de la economía.

Debido a lo antes expuesto la gobernanza de Internet tiene un papel muy importante. Sus puntos principales son:

- El grado en el cual la autoridad tiene capacidad para tomar decisiones.
- El nivel en que estas decisiones se implementan.
- La medida en la cual se alcanzan los objetivos que se han pretendido o, en su caso, se resuelven los problemas que se puedan presentar.
- La capacidad de hacer inteligibles las decisiones, es decir, de plantear y entender los problemas y las opciones disponibles.

### 4.5.3 Multistakeholder

Multistakeholder o múltiples partes interesadas se aplica principalmente en la gobernanza del Internet y es la participación de todos los sectores involucrados en el desarrollo y alcance de los objetivos planteados. Los sectores involucrados en el sistema multistakeholder son los siguientes:

- Sector público.
- Sector privado.
- La sociedad civil.
- La comunidad técnica.
- Las universidades.

Todos estos sectores adoptan resoluciones, acuerdos, políticas leyes y reglamentos para el correcto desarrollo de la sociedad del conocimiento. Así mismo se debe tener claro que el éxito o fracaso del resultado depende de todos los actores involucrados. De esta manera se busca obtener la mejor planificación y estrategia para obtener un objetivo en común. (Quezada 2017).

#### 4.5.3.1 Neutralidad de la red

La neutralidad de la red es el trato isonómico (igualdad ante la ley) que se le da a cualquier paquete de datos, sin distinción por contenido, origen y destino, servicio, terminal o aplicación. En palabras más sencillas significa que los “cables no tienen capacidad de decidir que circula por ellos”. Es decir que la información puede transmitirse sin necesidad de hacer distinción en el contenido que es transmitido. (Delgado 2014).

Desde sus inicios, el flujo de todo el contenido de Internet fue tratado sin ningún tipo de discriminación, así mismo sin importar si esta provenía de una empresa emergente (nueva) o multinacional. No se necesitaba permiso o poder de mercado para innovar en Internet y esta ha sido reconocido como una de sus principales fortalezas. El Consejo de Derechos Humanos de las Naciones Unidas reconoció la naturaleza abierta y global del Internet como una fuerza que impulsa el progreso hacia el desarrollo en sus varias formas para los países y la sociedad del conocimiento. (Delgado, 2014).

## 5. Metodología

Para el presente análisis se aplicará una investigación analítica descriptiva de los principales ciberataques, así como su influencia para la generación de políticas públicas de la gobernanza del Internet.

Ecuador ha sido objeto de varios ciberataques y estos han afectado los servicios públicos y las infraestructuras críticas (IC) dando como resultado la conmoción, preocupación y retraso en las actividades del país y sus ciudadanos.

En este trabajo de investigación se indagaron los ciberataques que han tenido un mayor impacto en términos de paralización de servicios críticos y en la generación de una conmoción social significativa que los llevó a ser ampliamente conocidos por la sociedad ecuatoriana. A continuación, se detallarán específicamente estos ataques de gran magnitud.

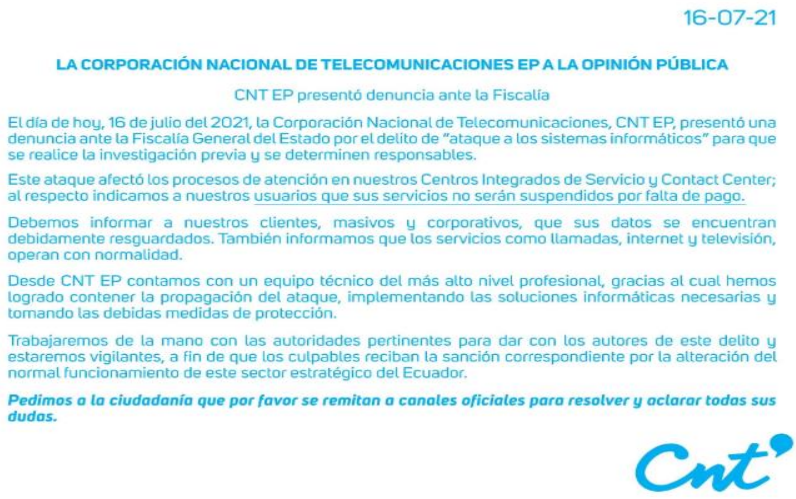
### 5.1 Ataques a instituciones públicas y privadas

#### 5.1.1 Ataque a la Corporación Nacional de Telecomunicaciones

El día 16 de Julio del año 2021, la Corporación Nacional de Telecomunicaciones fue víctima de un ciberataque. Este ataque fue anunciado por CNT en su página WEB dando a conocer que presentó la denuncia a la fiscalía.

**Figura 3**

Anuncio de CNT en su página WEB



16-07-21

**LA CORPORACIÓN NACIONAL DE TELECOMUNICACIONES EP A LA OPINIÓN PÚBLICA**

CNT EP presentó denuncia ante la Fiscalía

El día de hoy, 16 de julio del 2021, la Corporación Nacional de Telecomunicaciones, CNT EP, presentó una denuncia ante la Fiscalía General del Estado por el delito de "ataque a los sistemas informáticos" para que se realice la investigación previa y se determinen responsables.

Este ataque afectó los procesos de atención en nuestros Centros Integrados de Servicio y Contact Center; al respecto indicamos a nuestros usuarios que sus servicios no serán suspendidos por falta de pago.

Debemos informar a nuestros clientes, masivos y corporativos, que sus datos se encuentran debidamente resguardados. También informamos que los servicios como llamadas, internet y televisión, operan con normalidad.

Desde CNT EP contamos con un equipo técnico del más alto nivel profesional, gracias al cual hemos logrado contener la propagación del ataque, implementando las soluciones informáticas necesarias y tomando las debidas medidas de protección.

Trabajaremos de la mano con las autoridades pertinentes para dar con los autores de este delito y estaremos vigilantes, a fin de que los culpables reciban la sanción correspondiente por la alteración del normal funcionamiento de este sector estratégico del Ecuador.

***Pedimos a la ciudadanía que por favor se remitan a canales oficiales para resolver y aclarar todas sus dudas.***

Cnt

*Fuente:* Página web de CNT

Se tiene conocimiento que el virus ransomware EXX produjo el ataque esto debido a la publicación realizada en el sitio web Bleeping Computer por el investigador de seguridad Germán Fernández, quien mostro la página oculta que se tuvo acceso al momento dela incursión. (Abrams, 2021).

**Figura 4**

Mensaje del ataque efectuado por el virus Ransom EXX


*Fuente:* Imagen obtenida de página web Bleeping Computer

Este ciberataque indica que la CNT se encuentra continuamente bajo amenaza y a pesar que su data center es TIER III se puede confirmar que su ataque fue altamente efectivo y con tecnología especializada. (Ndavalos&Ndavalos, 2021).

### 5.1.2 Ataque a la Agencia Nacional de Tránsito

El día 20 de octubre del año 2021, la Agencia Nacional de Transito (ANT) sufrió un ciberataque. Dicho ataque fue reportado por el diario La Hora y este ataque afecto el sistema de entrega de licencias y matriculación vehicular.

A pesar que la ANT informó que los datos de los usuarios no fueron comprometidos porque tuvieron una actualización en sus sistemas de ciberseguridad, queda en evidencia la vulnerabilidad más aún cuando tuvieron recientemente una mejoría en sus sistemas.

Dicho ciberataque presentó una amenaza a la base de datos porque modifican los puntos de licencia, matriculación vehicular y turnos ya agendados. Este tipo de afectación y los continuos problemas de corrupción supone que el ataque lo realizo un ex trabajador como represalia a la institución. (La Hora, 2023).

### 5.1.3 Ataque a Banco Pichincha

El 11 de octubre del año 2021 el banco Pichincha informó sobre un incidente de ciberseguridad que provocó que los usuarios no puedan realizar transacciones en los canales electrónicos ni servicios en línea.

**Figura 5**

Declaraciones del Banco Pichincha


*Fuente:* Página web del Banco Pichincha

El Banco Pichincha es el mayor banco privado del Ecuador, esto lo hace un objetivo potencial para ciberataques. Debido a esto el banco tiene una infraestructura de seguridad estandarizados acorde a los de una institución financiera. A pesar de aquello el banco es objeto de ciberataques continuamente. (Sandoval, 2021).

Según información del sitio web Bleeping Computer indica que el ataque se trataría de un ransomware y que provocó la caída de la mayoría de los servicios bancarios. (Abrams, 2021).

### 5.1.4 Ataque Municipio de Quito

El 18 de abril del año 2022, la página SWISSINFO informó que el Municipio de Quito sufrió un ciberataque que afecto entre el 15 % y 20 % de su información, el objetivo principal fue la de inhabilitar el archivo digital.

Dicho ataque se habría realizado por medio de un virus ransomware – blackCat que buscaba acceder y encriptar toda la información ocasionando la caída de sus servicios. Además, es muy usual que los archivos encriptados tengan mensaje informando el posterior acceso a los archivos a cambio de dinero electrónico o criptomonedas.

En este caso los ingenieros de sistema del municipio de Quito tomaron la decisión de desconectar los servidores hasta poder realizar la desinfección de los equipos. A pesar que el municipio de Quito tiene una infraestructura de seguridad acorde para prevenir los ciberataques, este evento provocó la afectación a los 1.200 trámites que se procesan en el municipio. (Swissinfo, 2022).

### 5.1.5 Ataque al Ministerio de Salud Pública

Mediante un foro del mercado negro se dio a conocer el día 5 de marzo del año 2023, la venta de la base de datos de COVID-19 de los ecuatorianos del periodo 2021 a 2023, por parte del usuario kelvinsecurity. Dicha información se dio a conocer en la página web muchohacker. (Mucho Hacker, 2023).

**Figura 6**

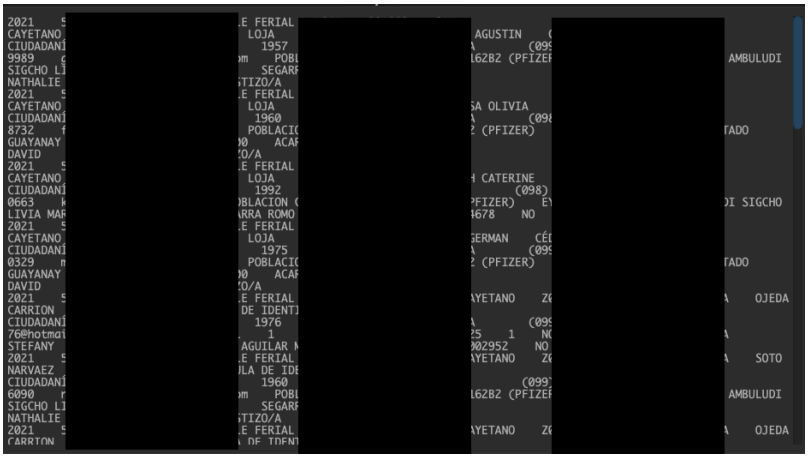
Mensaje del ciberatacante informando la venta de la base de datos


*Fuente:* Página web muchohacker

En el mismo foro el ciberatacante coloco una imagen donde consta 24 datos de ciudadanos con información de números de cedulas, nombres y apellidos completos entre otros. Mostrando así que la información es real y la misma contiene información sensible.

**Figura 7**

Parte del archivo con datos de los ciudadanos



*Fuente:* Página web muchohacker

Se conoce que la información del Ministerio de Salud Pública se encuentra respaldada conforme la normativa y protocolos internacionales de ciberseguridad. Sin embargo, el ministerio de Salud Pública informa que no existió vulneración de datos y que confíen en fuentes oficiales. (Mucho Hacker, 2023).

## 5.2 Políticas Públicas

### 5.2.1 Generación de políticas públicas en el Ecuador

Los ciberataques perpetrados al país ocasionaron inestabilidad a diversos sectores productivos y esto fue determinante para que el Ministerio de Telecomunicaciones gestionara la creación de políticas públicas para la protección de los usuarios. Así el Ecuador tendría herramientas legales para combatir y mitigar los ataques venideros.

Es así que el Ministerio de Telecomunicaciones crea las siguientes herramientas legales:

- La Ley Orgánica de Telecomunicaciones.
- La Ley Orgánica de Protección de Datos Personales.

#### 5.2.1.1 La Ley Orgánica de Telecomunicaciones

La ley Orgánica de Telecomunicaciones en el Título III Derechos y Obligaciones en su Capítulo I Abonados, clientes y usuarios en el artículo 22 inciso 4 dice:

"A la privacidad y protección de sus datos personales por parte del prestador con el que contrate servicios, con sujeción al ordenamiento jurídico vigente".

Este inciso garantiza la privacidad de sus datos personales para sus abonados y usuarios. Además, compromete al prestador de servicios que su seguridad sea la adecuada para cumplir con lo establecido.

Así mismo en el Capítulo II Prestador de servicios de Telecomunicaciones, en su artículo 24 Obligaciones de los prestadores de servicios de telecomunicaciones inciso 14 dice:

"Adoptar las medidas necesarias para la protección de los datos personales de sus usuarios y abonados, de conformidad con esta ley, su reglamento general y las normas técnicas y regulaciones respectivas".

Este inciso obliga a los prestadores de servicios de telecomunicaciones que tomarán todas las medidas necesarias para proteger los datos de sus usuarios y abonados.

En el artículo 79 del Capítulo II Deber de información dice:

"En caso de que exista un riesgo particular de violación de la seguridad de la red pública o del servicio de telecomunicaciones, el prestador de servicios de telecomunicaciones informará a

sus abonados, clientes y usuarios sobre dicho riesgo y sobre las medidas a adoptar. En caso de violación de los datos de un abonado o usuario particular, el prestador notificará de tal violación al abonado o usuario particular en forma inmediata, describiendo al menos la naturaleza de la violación de los datos personales, los puntos de contacto donde puede obtenerse más información, las medidas recomendadas para atenuar los posibles efectos adversos de dicha violación y las medidas ya adoptadas frente a la violación de los datos personales. La notificación de una violación de los datos personales a un abonado, cliente o usuario particular afectado no será necesaria si el prestador demuestra a la Agencia de Regulación y Control de las Telecomunicaciones que ha aplicado las medidas de protección tecnológica convenientes y que estas medidas se han aplicado a los datos afectados por la violación de seguridad. Unas medidas de protección de estas características convierten los datos en incomprensibles para toda persona que no esté autorizada a acceder a ellos. A los efectos establecidos en este artículo, se entenderá como violación de los datos personales la violación de la seguridad que provoque la destrucción, accidental o ilícita, la pérdida, la alteración, la revelación o el acceso no autorizados, de datos personales transmitidos, almacenados o tratados en la prestación de un servicio de telecomunicaciones.”.

#### 5.2.1.2 La ley Orgánica de Protección de Datos Personales

La ley Orgánica de Protección de Datos Personales en su Capítulo I Ámbito de Aplicación Integral, Artículo 1 Objeto y finalidad dice:

“El objeto y finalidad de la presente ley es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos personales, que incluye el acceso y decisión sobre información y datos de carácter, así como su correspondiente protección. Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela.”.

En su Capítulo II Principios, articulo 10 literal j dice:

“Seguridad de datos personales. - Los responsables y encargados de tratamiento de los datos personales deberán implementar todas las medidas de seguridad adecuadas y necesarias, entendiéndose por tales las aceptadas por el estado de la técnica, sean estas organizativas, técnicas o de cualquier otra índole, para proteger los datos personales frente a cualquier riesgo, amenaza, vulnerabilidad, atendiendo a la naturaleza de los datos de carácter personal, al ámbito y el contexto”.

Este literal indica que los responsables del tratamiento de los datos personales realizaran todas las implementaciones y técnicas para proteger los datos ante cualquier riesgo o amenaza.

En su Capítulo VI Seguridad de datos personales, artículo 37 dice:

"Seguridad de datos personales. - El responsable o encargado del tratamiento de datos personales según sea el caso, deberá sujetarse al principio de seguridad de datos personales, para lo cual deberá tomar en cuenta las categorías y volumen de datos personales, el estado de la técnica, mejores prácticas de seguridad integral y los costos de aplicación de acuerdo a la naturaleza, alcance, contexto y los fines del tratamiento, así como identificar la probabilidad de riesgos.

El responsable o encargado del tratamiento de datos personales, deberá implementar un proceso de verificación, evaluación y valorización continua y permanente de la eficiencia, eficacia y efectividad de las medidas de carácter técnico, organizativo y de cualquier otra índole, implementadas con el objeto de garantizar y mejorar la seguridad del tratamiento de datos personales.

El responsable o encargado del tratamiento de datos personales deberá evidenciar que las medidas adoptadas e implementadas mitiguen de forma adecuada los riesgos identificados.

Entre otras medidas, se podrán incluir las siguientes:

1) Medidas de anonimacion, seudionomizacion o cifrado de datos personales;

2)Medidas dirigidas a mantener la confidencialidad, integridad y disponibilidad permanentes de los sistemas y servicios del tratamiento de datos personales y el acceso a los datos personales, de forma rápida en caso de incidentes; y

3) Medidas dirigidas a mejorar la resiliencia técnica, física, administrativa y jurídica.

4)Los responsables y encargados del tratamiento de datos personales, podrán acogerse a estándares internacionales para una adecuada gestión de riesgos enfocada a la protección de derechos y libertades, así como para la implementación y manejo de sistemas de seguridad de la información o a códigos de conducta reconocidos y autorizados por la Autoridad de Protección de datos Personales".

En su artículo 38 dice:

"Medidas de seguridad en el ámbito del sector público. - El mecanismo gubernamental de seguridad de la información deberá incluir las medidas que deban implementarse en el caso de

tratamiento de datos personales para hacer frente a cualquier riesgo, amenaza, vulnerabilidad, accesos no autorizados, pérdidas, alteraciones, destrucción o comunicación accidental o ilícita en el tratamiento de los datos conforme al principio de seguridad de datos personales.

El mecanismo gubernamental de seguridad de la información abarcara y aplicara a todas las instituciones del sector público, contenidos en el artículo 225 de la Constitución de la República del Ecuador, así como a terceros que presten servicios públicos mediante concesión u otras figuras legalmente reconocidas. Estas, podrán incorporar medidas adicionales al mecanismo gubernamental de seguridad de la información."

En este artículo se da a conocer que se debe implementar medidas para hacer frente a cualquier vulneración de seguridad y las empresas que presten servicios públicos en concesión deberán incorporar medidas adicionales al ya establecido.

En su artículo 43 dice:

"Notificación de vulneración de seguridad.- El responsable del tratamiento deberá notificar la vulneración de la seguridad de datos personales a la Autoridad de Protección de Datos Personales y la Agencia de Regulación y Control de Telecomunicaciones, tan pronto sea posible, y a más tardar en el término de cinco (5) días después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de protección de datos no tiene lugar en el término de cinco (5) días, deberá ir acompañada de indicación de los motivos de la dilación.

El encargado del tratamiento deberá notificar al responsable cualquier vulneración de la seguridad de datos personales tan pronto sea posible, y a más tardar dentro del término de dos (2) días contados a partir de la fecha en la que tenga conocimiento de ella. "

En el artículo indica que, si existió una vulneración de seguridad, el responsable deberá notificar de la vulneración a los organismos competentes tan pronto sea posible.

Estas políticas nos ayudan en la protección de nuestra información y datos personales sin embargo existe penalidad al cometer estos ciberdelitos que afectan las infraestructuras críticas y perjudican al país. Estas penalidades las encontramos en el COIP (Código Orgánico Integral Penal).

**Tabla 1**

Delitos tipificados en el COIP

| TIPIFICACION | Art. | TIPO PENAL | PENA PRIVATIVA |
|---|---|---|---|
| Revelación ilegal de información en base de datos | 229 | Revelación ilegal de base de datos | 1 a 3 años |
| Intercepción ilegal de datos | 230 | Interceptación ilegal de base de datos | 3 a 5 años |
| Fraude informático y muleros | 231 | Transferencia electrónica de activo patrimonial | 3 a 5 años |
| Daños informáticos, Malware, ataques de DoS y DDoS | 232 | Ataque a la integridad de sistemas informáticos | 3 a 5 años |
| Delitos contra la información pública reservada | 233 | Delitos contra la información pública reservada legalmente | 5 a 7 años |
| Acceso no autorizado a sistemas informáticos, telemáticos o de telecomunicaciones | 234 | Acceso no consentido a un sistema informático, telemático o de telecomunicaciones | 3 a 5 años |

*Fuente: COIP*

## 5.3 Gobernanza del Internet

### 5.3.1 Gobernanza del Internet en Ecuador

El Internet hoy en día es una herramienta necesaria para el desarrollo de la sociedad, una prueba de aquello es que el acceso a la información es un derecho constitucional. Es por eso que el gobierno nacional tiene como compromiso garantizar que el acceso a la información sea seguro, privado y de libre acceso.

La gobernanza del Internet para que sea efectiva debe de existir un compromiso y colaboración de todos los involucrados en la gestión y desarrollo. Esto quiere decir que el sector del gobierno, el sector privado, la sociedad civil y el sector académico, reconocen sus funciones y responsabilidades en beneficio del Internet.

El Foro de Gobernanza de Internet del Ecuador desde el año 2012 ha realizado consultas a través de foros con todos los actores involucrados. Esto conlleva a que cada tema tratado recibe un feedback de parte de los involucrados en el foro dando consigo una propuesta de mejoría de parte de todos los involucrados en el ecosistema.

El foro de gobernanza de Internet del Ecuador es reconocido por la Secretaría de las Naciones Unidas como un IGF nacional es así que toma los principios y procedimientos básicos de un IGF. (IGF 2021).

#### 5.3.1.1 Modelo Multistakeholder (múltiples partes)

Para que existe una gobernanza es necesario la participación de todas los involucrados en el ecosistema, es decir el modelo Multistakeholder consiste en que todas las partes interesadas participan, ponen a consideración su aporte y conocimiento para el desarrollo del ecosistema del Internet.

El modelo de múltiples partes interesadas es una manera de hacer las cosas que se puede usar en cualquier situación. Sea para resolver un problema o para ayudar en el desarrollo y evolución de una institución.

### 5.3.2 Estrategia Nacional de Ciberseguridad

En el Ecuador debido a los ciberataques perpetrados donde se han visto involucrados el sector de telecomunicaciones, entidades financieras, de trasporte y gobiernos autónomos. La actual

ministra de Telecomunicaciones con ayuda del programa de Ciberseguridad del Comité Interamericano contra el Terrorismo, la Organización de Estados Norteamericanos (CICTE/OEA) y al proyecto de Resiliencia Cibernética para el Desarrollo, de la Unión Europea (CYBER4DEV), elaboro la Estrategia Nacional de Ciberseguridad. La Estrategia Nacional de Ciberseguridad es un claro ejemplo que se ha trabajado en un modelo multistakeholder, esto debido a que se invitó a muchas partes interesadas que forman parte de los actores del estado. (Maino, 2022).

Esta estrategia tuvo la participación de actores de la sociedad civil, del sector académico, expertos en ciberseguridad, funciones del estado, sector privado y de las instituciones que conforman el Comité Nacional de Ciberseguridad. Este organismo fue creado en el gobierno de Guillermo Lasso y está conformada por representantes del Ministerio de Telecomunicaciones y de la sociedad de la Información, Defensa Nacional, Gobierno, Interior, Relaciones exteriores y Movilidad Humana, así como el centro de Inteligencia estratégica y la Secretaria General de la Administración Pública de la Presidencia. (Maino, 2022).

La estrategia Nacional de Ciberseguridad tendrá una aplicación de tres años (2022 – 2025) y esta consta de 6 pilares fundamentales que son:

- Gobernanza y coordinación nacional
- Resiliencia cibernética
- Prevención y lucha contra la cibercriminalidad
- Ciberdefensa nacional
- Habilidades y capacidades de ciberseguridad
- Cooperación internacional

## 6. Resultados

Los continuos ataques a las instituciones públicas y privadas tuvieron su repercusión; ya que el Ministerio de Telecomunicaciones gestionó de forma coordinada y efectiva la creación de La Estrategia Nacional de Ciberseguridad del Ecuador, permitiendo así la participación de expertos, la sociedad civil, académicos, sector público y privado para lograr mediante el modelo multistakeholder un aporte y colaboración efectiva para el desarrollo y protección del ecosistema del internet. Esta estrategia fue aprobada por el Comité Nacional de Ciberseguridad el 3 de agosto del año 2022. Desde esa fecha se tiene a disposición una herramienta efectiva para la protección de los ciberataques y la misma fue desarrollada con altos estándares internacionales. Sin embargo, él Ecuador actualmente está ubicado en el puesto # 42 de países con más ciberamenazas a nivel mundial. Y en Latinoamérica y el Caribe ocupamos el puesto # 4 según información del mapa de riesgo de la empresa Kaspersky.

Ecuador es uno de los países con más ciberamenazas, y a su vez es uno de los países más perpetrados, esto debido a la falta de políticas públicas.

En el Ecuador, a pesar que se ha hecho desde el 2012 cada año constantemente mesas de gobernanza de Internet, todavía no se tiene una política de gobernanza de Internet como lo tienen en otros países.

Muchos de los ataques que se han hecho a grandes escalas y ha instituciones públicas o privadas que son de gran relevancia en el Ecuador, no se ha divulgado porque se busca precautelar la reputación de dicha institución.

# 7. Discusión

## 7.1. Contrastación empírica

Los ciberataques perpetrados a las empresas públicas y privadas permitieron agilitar la creación de la Estrategia Nacional de Ciberseguridad, cuya herramienta representa un gran avance en políticas de ciberseguridad. Ya que se tenía como herramientas legales la Ley Orgánica de Protección de Datos Personales y la Ley Orgánica de Telecomunicaciones, sin embargo, no estaban enfocadas en la seguridad del ciberespacio.

Sin embargo, la estrategia Nacional de Seguridad debe ser continuamente actualizada a medida que aparezcan nuevas tecnologías que faciliten los ciberataques haciéndolos más eficaces.

## 7.2 Limitaciones

El estudio realizado tiene como limites las fuentes de información especializadas que notifican los ciberataques. Esto debido al sigilo que tienen las empresas afectadas al momento de informar el ataque perpetrado. Además de que existen medios de comunicación que informan de manera sesgada a la ciudadanía.

Otra limitante que se encontró fue el poco conocimiento que se tiene a los temas de políticas públicas. Esto debido a que el Ecuador es uno de los países que recién ha tomado en cuenta el tema de las políticas públicas para el ciberespacio. Entonces no se cuenta documentación técnica, es decir los abogados y sociólogos comentan sobre las políticas públicas pero muy pocos ingenieros analizan y comentan del tema.

## 7.3 Aspectos importantes

El estudio de los ciberataques, su influencia a las políticas públicas, así como la gobernanza del Internet representan un análisis extenso. Esto debido a la naturaleza que implica la gobernanza del Internet porque implica desde la estructura del diseño de red, sus protocolos, su hardware y personal especializado. Es decir, involucra a todos los componentes que hacen que el Internet sea posible.

Como un aspecto importante se destaca el hecho que el Ecuador implementó la estrategia Nacional de Ciberseguridad, permitiendo obtener una mejor herramienta para la defensa a los ciberataques, así como una continua revisión a la herramienta legal, esto con el fin de realizar una permanente actualización cuando sea necesario.

Otro aspecto importante es la inclusión en el Código Orgánico Integral Penal (COIP) de los ciberdelitos. Con esto se tiene tipificado los ciberdelitos, así como su respectiva penalización.

## 8. Conclusiones

Los ciberataques perpetrados a las infraestructuras críticas y empresas privadas permitieron agilizar la creación de políticas públicas dando como resultado la creación de La Estrategia Nacional de Ciberseguridad.

El confinamiento producto de la pandemia del Covid-19 nos obligó a desarrollar y aprender nuevas formas de trabajo como el teletrabajo, esta acción expuso las vulnerabilidades que presentan las empresas en su diseño de red y ciberseguridad.

La Estrategia Nacional de Ciberseguridad es una metodología esencial para la protección y uso del ciberespacio, es por eso que se necesita que sea continuamente revisada y analizada por los miembros que componen la gobernanza del Internet en el país.

La Estrategia Nacional de Ciberseguridad es una herramienta esencial, sin embargo, su efectividad dependerá del compromiso del Comité Nacional de Ciberseguridad y de las instituciones encargadas de la seguridad en el país.

Se confirma la relación directa que tiene el ciberespacio con la vida cotidiana, esto debido a que los ciberataques afectan las actividades y el normal desarrollo de la sociedad civil.

La implementación de la Estrategia Nacional de Ciberseguridad confirma que el país tiene un buen inicio en materia de Ciberseguridad sin embargo existe mucho camino por recorrer.

## 9. Recomendaciones

Se recomienda la capacitación continua del personal especializado que conforma el Comité Nacional de Ciberseguridad, esto con el fin de plantear modificaciones y mejoras a los objetivos planteados en la Estrategia Nacional de Ciberseguridad.

Se recomienda que las universidades que ofrecen las carreras de telecomunicaciones incluyan en su malla curricular la materia de marco regulatorio y políticas públicas de las telecomunicaciones.

Se recomienda la creación de un departamento de control y monitoreo que evalué la operatividad de todas las infraestructuras críticas del país y que la misma sea las 24 horas y todos los días del año.

Se recomienda la creación de un mecanismo que realice un efectivo seguimiento a los Proveedores de Servicios de Internet (ISP) para que cumplan con la normativa ya estipulada en el Ecuador como son la Ley Orgánica de Protección de Datos Personales y la Ley Orgánica de Telecomunicaciones.

Se recomienda una campaña agresiva en los medios de comunicación sobre la concientización de normas de ciberseguridad. Esto con el fin de lograr que la ciberseguridad sea una habito cotidiano.

Se recomienda una campaña para la concientización de las mesas de Gobernanza de Internet, esto con el fin de que la ciudadanía conozca más del tema.

## 10. Bibliografía


Catota, F. E., Morgan, M. G., &Sicker, D. (2018). Cybersecurity incident response capabilities in the Ecuadorian financial sector. *Journal of Cybersecurity*, *4*(1). https://doi.org/10.1093/cybsec/tyy002

Alvarado, J. E. A. C. (2020, mayo). ANÁLISIS DE ATAQUES CIBERNÉTICOS HACIA EL ECUADOR. Revista Científica Aristas. https://revistacientificaistjba.edu.ec/images/joomgallery/details/gallery_2/gallery_1_9/Edicion_Mayo_2020_COMPLETO-c.pdf#page=19

Data explorer - ITU DataHub. (2022). https://datahub.itu.int/data/?e=ECU

C. (2022, 9 mayo). Diferencias entre ciberataques activos y pasivos. Ciberseguridad. https://ciberseguridad.com/amenzas/ciberataques-activos-pasivos/

A. (2021, 24 octubre). ¿Qué es un ataque activo? (Actualizado 2023). Krypton Solid. https://kryptonsolid.com/que-es-un-ataque-activo/

Gobernanza de Internet. (2023, 1 febrero). UNESCO. https://www.unesco.org/es/internet-governance

C. (2022a, febrero 28). Ciberespacio: definición, aplicaciones y límites. Ciberseguridad. https://ciberseguridad.com/guias/recursos/ciberespacio/

¿Qué es un ciberataque? | IBM. (2023).https://www.ibm.com/es-es/topics/cyber-attack

T. (2019). X.800A. A Security architecturefor Open SystemsInterconnectionfor CCITT applications.https://www.itu.int/rec/T-REC-X.800/en

Universidad Complutense de Madrid. (2016, 10 noviembre). https://www.ucm.es/data/cont/docs/72-2016-11-10-1+Introduccio%CC%81n.pdf

Bertolín, J. A. (2020). Búsqueda y hallazgo de confluencias esenciales entre actividades hostiles y contramedidas en ciberseguridad. Dialnet. https://dialnet.unirioja.es/servlet/articulo?codigo=7685958

Las políticas públicas y la gestión pública: un análisis desde la teoría y la práctica. (2019.-b).https://revistas.uasb.edu.ec/index.php/eg/article/download/1207/1125?inline=1

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2022, 22 agosto). Por primera vez Ecuador cuenta con su Estrategia Nacional de Ciberseguridad – Ministerio de Telecomunicaciones y de la Sociedad de la Información. Recuperado 25 de marzo de 2023, de https://www.telecomunicaciones.gob.ec/por-primera-vez-ecuador-cuenta-con-su-estrategia-nacional-de-ciberseguridad/

Sobre la Unión Internacional de Telecomunicaciones (UIT). (2023). ITU. https://www.itu.int/es/about/Pages/default.aspx

Quienes Somos. (2023). OEA.ORG. Recuperado 25 de marzo de 2023, dehttps://www.oas.org/es/acerca/quienes_somos.asp

Políticas públicas de Sociedad de la Información en América Latina: ¿una misma visión? (2010, marzo). https://www.cepal.org/SocInfo. Recuperado 25 de marzo de 2023, de https://repositorio.cepal.org/bitstream/handle/11362/3757/1/S2010178.pdf

Leyva-Méndez, A. E. (2021, 12 marzo). Open Journal Systems. https://polodelconocimiento.com/ojs/index.php/es/article/view/2431/5017

Tapuia. (2005). https://tapuia.blog.br/sites/default/files/2023-01/C+Afonso+-+Gobernanza+de+Internet+-+jul+2005.pdf

Google Libros. (2008, 1 julio). FundacionTelefonica. Recuperado 25 de marzo de 2023, de https://books.google.com/?hl=es

Quezada, V. F. W. (2017, 8 diciembre). DSpace en ESPOL: Análisis de la gobernanza de internet en el entorno mundial y su impacto en Ecuador. https://www.dspace.espol.edu.ec/handle/123456789/41821

Delgado, J. A. (2014, noviembre). Gobernanza de Internet en Ecuador: Infraestructura y acceso. Artículo presentado en el Encuentro Nacional de Gobernanza de Internet, Quito, Ecuador. Obtenido de http :// delgado. ec/ research/ es/ Gobernanza _ Internet _ Ecuador _2014. pdf

Índice Mundial de Ciberseguridad 2020. (2021). ITU. Recuperado 30 de marzo de 2023, de https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Comisión Europea. (2014, 2 enero). Políticas públicas de la sociedad de la información en América Latina: ¿una misma visión?https://repositorio.cepal.org/handle/11362/3757

Morán, D. R. (2015). La visión internacional de la ciberseguridad. Dialnet. https://dialnet.unirioja.es/servlet/articulo?codigo=7685503

Abrams, L. (2021, 3 agosto). Ecuador's state-run CNT telco hit by RansomEXX ransomware.BleepingComputer. https://www.bleepingcomputer.com/news/security/ecuadors-state-run-cnt-telco-hit-by-ransomexx-ransomware/

https://sensorstechforum.com/es/remove-exx-ransomware/

Ndavalos, &Ndavalos. (2021).Los misterios del ataque que dejó a CNT sumida en la “emergencia” Primicias. https://www.primicias.ec/noticias/tecnologia/los-misterios-del-ataque-que-dejo-a-cnt-sumida-en-emergencia/

Ciberataque a ANT detiene trámite de licencias y matrículas. (2021). https://www.lahora.com.ec/pais/tramites-ant-suspendidos-ciberataque/

Sandoval, P. (2021, 20 octubre). Ciberataque a Banco Pichincha fue realizado por atacantes internacionales, se revela en Comisión de Desarrollo Económico. .Economía | Noticias | El Universo.https://www.eluniverso.com/noticias/economia/ciberataque-a-banco-pichincha-fue-realizado-por-atacantes-internacionales-se-revela-en-comision-de-desarrollo-economico-nota/

Abrams, L. (2021b, octubre 12). Cyberattack shuts down Ecuador's largest bank, Banco Pichincha. BleepingComputer. https://www.bleepingcomputer.com/news/security/cyberattack-shuts-down-ecuadors-largest-bank-banco-pichincha/

El Municipio de Quito, víctima de ciberataque que afectó el 15 % de sus datos.(2022, 18 abril). SWI swissinfo.ch. https://www.swissinfo.ch/spa/ecuador-ciberataque_el-municipio-de-quito--v%C3%ADctima-de-ciberataque-que-afect%C3%B3-el-15---de-sus-datos/47525602

H. (2023, 6 marzo). Ponen a la venta base de datos con información sensible de todos los ecuatorianos vacunados contra Covid 19. MuchoHacker.LOL. https://muchohacker.lol/2023/03/ponen-a-la-venta-base-de-datos-con-informacion-sensible-de-todos-los-ecuatorianos-vacunados-contra-covid-19/

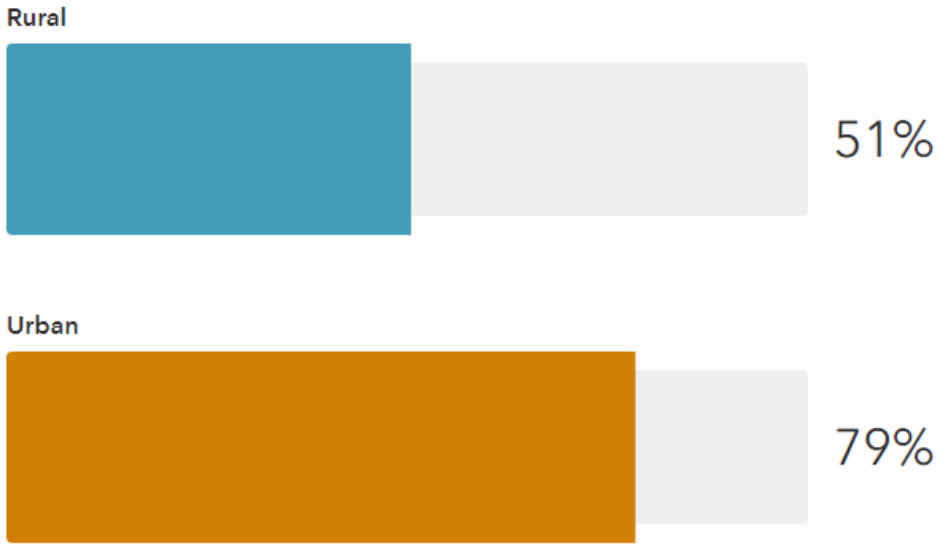
Quienes somos – IGF ECUADOR. (2021, 9 junio). https://igfecuador.ec/2021/06/09/quienes-somos/

Frankie E Catota, M Granger Morgan, Douglas C Sicker, Cybersecurityincident response capabilities in theEcuadorianfinancial sector, JournalofCybersecurity, Volume 4, Issue 1, 2018, tyy002, https://doi.org/10.1093/cybsec/tyy002

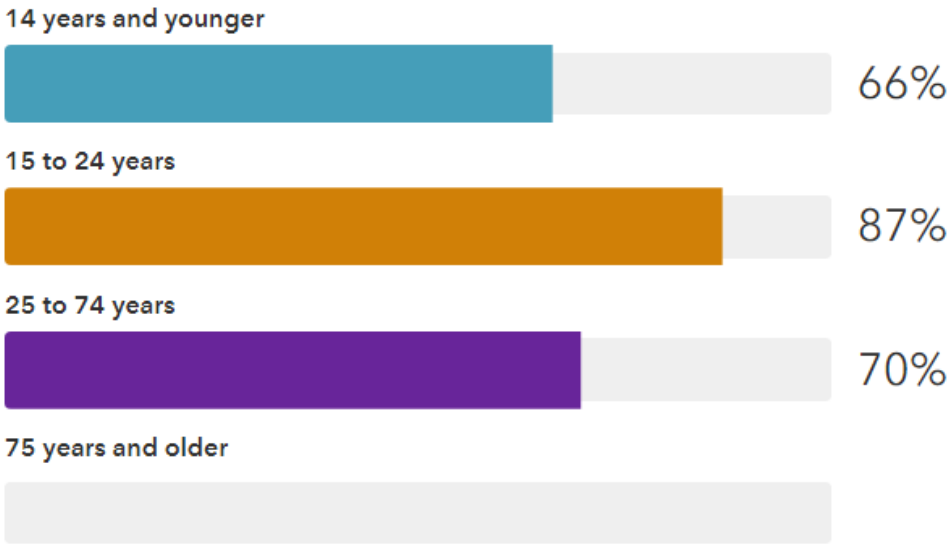
Maino, V. M. (2022, agosto). ESTRATEGIA NACIONAL DE CIBERSEGURIDAD DEL ECUADOR. Asobanca. https://asobanca.org.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-DEL-ECUADOR-2022481.pdf

## 11. Anexos

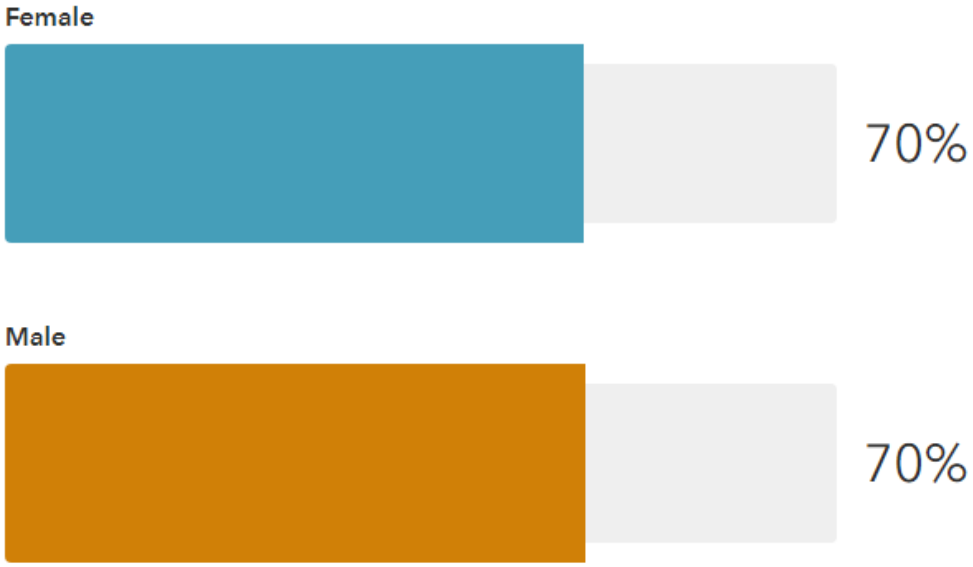
**Anexo 1.**Porcentaje de usuarios de la zona rural y urbana que usan el internet en el Ecuador según información de la ITU del año 2022.




**Anexo 2.**Porcentaje de usuarios por edad que usan el internet en el Ecuador según información de la ITU del año 2022.



**Anexo 3.** Porcentaje de usuarios clasificados por género que usan el internet en el Ecuador según información de la ITU del año 2022.



**Anexo 4.** Certificación de traducción del resumen

CERTIFICADO DE TRADUCCION

CERTIFICO:

Haber realizado la traducción de español al inglés del resumen de la tesis titulada: Análisis de la influencia de los ciberataques para la generación de políticas públicas en el Ecuador en el ámbito de la gobernanza del Internet.¨, de autoría ING. HUGO ERNESTO ACARO GALLEGOS con cedula número 0921405692, egresado de la facultad de la Energía, las Industrias y los Recursos Naturales no Renovables de la Universidad Nacional de Loja, trabajo que se encuentra bajo la dirección del Ing. John Jossimar Tucker Yépez, Mg. Sc. Previo a la obtención del título de Magister en Telecomunicaciones.

Es todo cuanto puedo certificar en honor a la verdad, facultando al interesado hacer del presente en lo que creyere conveniente.

Cuenca, 12 de mayo de 2023

Catherine M. Vicente

ATIEC member #22

ID 0103877015

Cellular (593)999860667

Email: cathyvicente@hotmail.com