UIDE

Powered by
Arizona State University

RELACIONES INTERNACIONALES

Disertación previa a la obtención del título de Licenciado en Relaciones Internacionales.

AUTOR: Jennifer Crespo

TUTOR: MSc. Diana Gabriela Rosas Lanas

Influencia de la Guía para la Elaboración de una Estrategia Nacional de Ciberseguridad (2018) de la UIT en la adopción de políticas de ciberseguridad, durante el periodo 2018 – 2021. Los casos de Colombia y Ecuador.

CERTIFICACIÓN DE AUTORÍA

Yo, Jennifer Adriana Crespo Arévalo, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido presentado anteriormente para ningún grado o calificación profesional y que se ha consultado la bibliografía detallada.

Cedo mis derechos de propiedad intelectual a la Universidad Internacional del Ecuador, para que sea publicado y divulgado en internet, según lo establecido en la Ley de Propiedad Intelectual, su reglamento y demás disposiciones legales.

Firmado electrónicamente por:
JENNIFER
ADRIANA CRESPO
AREVALO

C.I.: 0302322011

APROBACIÓN DEL TUTOR

Yo, Diana Gabriela Rosas Lanas, certifico que conozco al autor del presente trabajo siendo la responsable exclusiva tanto de su originalidad y autenticidad, como de su contenido.

Firmado electrónicamente por:
DIANA
GABRIELA
ROSAS LANAS

……

DIRECTOR DE TESIS

ACUERDO DE CONFIDENCIALIDAD

La Biblioteca de la Universidad Internacional del Ecuador se compromete a:

1. No divulgar, utilizar ni revelar a otros la **información confidencial** obtenida en el presente trabajo, ya sea intencionalmente o por falta de cuidado en su manejo, en forma personal o bien a través de sus empleados.

2. Manejar la **información confidencial** de la misma manera en que se maneja la información propia de carácter confidencial, la cual bajo ninguna circunstancia podrá estar por debajo de los estándares aceptables de debida diligencia y prudencia.

Dr. Arturo Moscoso	Gabriela Fernández
Director – Escuela de RRII	Gestora Cultural

Influencia de la Guía para la Elaboración de una Estrategia Nacional de Ciberseguridad (2018) de la UIT en la adopción de políticas de ciberseguridad, durante el periodo 2018 – 2021: los casos de Colombia y Ecuador.

Jennifer Adriana Crespo Arévalo

Tutora: MSc. Diana Gabriela Rosas Lanas

Resumen:

El empleo masivo de las TICs genera amplios beneficios socioeconómicos, pero también riesgos y amenazas que atentan contra la seguridad internacional, estatal, empresarial y ciudadana. Por tanto, la implementación de políticas de ciberseguridad es prioridad de los actores estatales y no estatales. En ese sentido, desde el neoliberalismo institucional, se explica la importancia de las instituciones internacionales en la adopción de políticas domésticas de ciberseguridad y, a partir de un ejercicio comparado, se identifican los aspectos de las políticas nacionales de Colombia y Ecuador, adoptadas entre 2018 y 2021, en los que influyó la UIT.

Abstract:

The massive use of ICTs generates broad socioeconomic benefits, but also risks and threats that affect international, state, business, and citizen security. Therefore, the implementation of cybersecurity policies is a priority for State and non-state actors. In this sense, from institutional neoliberalism, the importance of international institutions in the adoption of domestic cybersecurity policies is explained and based on a comparative exercise, the aspects of Colombia's, and Ecuador's national policies, adopted between 2018 and 2021, in which the ITU influenced, are identified.

1) Introducción

La cuarta revolución industrial permitió la expansión acelerada de las Tecnologías de la Comunicación y de la Información TICs, que generan amplios beneficios para los Estados, las organizaciones y las personas. Sin embargo, estas herramientas también propiciaron el desarrollo de nuevas amenazas y riesgos que vulneran los sistemas informáticos y las infraestructuras críticas -públicas y privadas-. Adicionalmente, los ciberataques ya no se efectúan únicamente por parte de los individuos o grupos pequeños, sino también por actores estatales, empresas y redes de delincuencia organizada transnacional (Ministerio de Defensa Nacional et. al., 2020; CONPES, 2020).

Bajo esas ideas, el ciberespacio representa un escenario con amenazas innovadoras que atentan contra las instituciones públicas y privadas, nacionales e internacionales y, contra el ejercicio de los derechos humanos. Por ende, la adopción de estrategias nacionales de ciberseguridad es de interés de la comunidad internacional y, principalmente, de las autoridades estatales. De ahí que, en el presente siglo, el fomento de la seguridad e integridad en el espacio cibernético sea una prioridad de las agendas globales, regionales y nacionales.

Con Resolución No. 56/183 de 2001, la ONU acordó desarrollar la Cumbre Mundial de la Sociedad de la Información -en adelante CMSI-, un foro de alto nivel en el que se delineó el rol de la Unión Internacional de Telecomunicaciones -en adelante UIT-, en el ámbito de ciberseguridad. Ya que, los líderes gubernamentales de dicha cumbre reconocieron a la UIT como el organismo que facilitaría la implementación de la línea de acción No. 5 del Plan de Acción de Ginebra, referente a la construcción de seguridad y confianza digital.

A fin de cumplir con mencionada responsabilidad, la UIT implementó un programa formativo de ciberseguridad, que proporciona a las autoridades estatales las

herramientas necesarias para potenciar las capacidades digitales indispensables para mejorar la seguridad cibernética. En este marco, en 2018, la UIT publicó la Guía para la Elaboración de una Estrategia Nacional de Ciberseguridad -en adelante la Guía-; con el objeto de guiar al Estado en la adopción de estrategias nacionales, concordantes con la realidad de cada país y las prácticas internacionales.

Por otra parte, las iniciativas estatales de ciberseguridad son recientes. Con el Documento CONPES 3701 de 2011, Colombia adoptó su primera política de ciberseguridad; a fin de incrementar las capacidades públicas para gestionar los ciberriesgos que amenazan la seguridad pública y la defensa nacional. Posteriormente, la fase de evaluación de dicho instrumento propició la reformulación de estrategias, ajustándolas cada vez a los modernos riesgos digitales. Consecuentemente, en 2016, el Estado colombiano implementó su segunda política nacional mediante el Documento CONPES 3854, que también fue evaluado y modificado en 2020, al adoptarse el Documento CONPES 3995, que contiene la política pública objeto del presente estudio.

Por su parte, el Estado ecuatoriano adoptó su primera política de ciberseguridad en 2021, con el objetivo de fortalecer las capacidades digitales necesarias para asegurar el adecuado ejercicio de los derechos humanos y la integridad de los bienes esenciales para el desarrollo nacional. Con este instrumento, Ecuador reconoce que la construcción de esquemas de seguridad digital demanda altos niveles de cooperación entre actores estatales y no estatales, nacionales e internacionales.

Con esos antecedentes, este trabajo estudia la influencia de la Guía para la Elaboración de una Estrategia Nacional de Ciberseguridad (2018) de la UIT en la adopción de políticas de seguridad digital en Colombia y Ecuador, durante el periodo 2018 – 2021. En otras palabras, se analiza la existencia de una relación de interdependencia entre la institución internacional y dos Estados, a partir de los

planteamientos de la teoría del institucionalismo neoliberal. Entendiendo que, aunque el Estado es el actor que define las relaciones en el sistema internacional, las instituciones cumplen un rol trascendental al incidir en el comportamiento estatal y en la política internacional (Stein, 2008).

2) Marco teórico

La teoría del neoliberalismo institucional estudia las instituciones internacionales; es decir, su desarrollo e importancia en los escenarios nacionales, regionales e internacionales. Para Keohane (1993), hasta cierto punto, dichos actores rigen el sistema internacional e inciden en el comportamiento estatal. Ya que, prestan asistencia a los Estados para encontrar soluciones a problemas sociales, económicos o políticos.

Según Keohane (1993), la anarquía internacional -inexistencia de un gobierno común- provoca que los Estados pongan a consideración sus intereses domésticos en la arena internacional; con el propósito de articularlos a través de la cooperación multilateral, que es propiciada por los organismos internacionales. En dicho contexto, estas instituciones son reglas de carácter formal o informal, que definen conductas y limitan la actividad estatal (Keohane, 1993). Igualmente, son acuerdos que permiten reducir los costos de actuar y solventar problemas públicos (Grieco & Ikenberry, 2002). De modo que, las instituciones internacionales guían la actuación estatal, mediante la adopción de agendas comunes con las que los Estados se comprometen.

Por su parte, Stein (2008) define a las instituciones internacionales como acuerdos que surgen de la voluntad estatal para construir agendas comunes, que de ser cumplidas generan amplios beneficios para el Estado. De ahí que, los estudios del neoliberalismo institucional se hayan centrado en analizar el cumplimiento de los

compromisos estatales asumidos con los organismos internacionales (Stein, 2008). Concluyendo que, los Estados cumplen dichos acuerdos, que generalmente no asumen como actor individual (Stein, 2008).

Ahora bien, las instituciones internacionales surgen para afrontar determinados problemas. En ese sentido, la UIT nació en 1865 para facilitar las comunicaciones; empero, el desarrollo tecnológico propició su evolución, hasta consolidarse como el organismo especializado para las TICs del Sistema de Naciones Unidas. Desde ese momento y bajo los lineamientos de la CMSI, esta institución internacional ha trabajado en la implementación de un marco de cooperación multilateral, que permita construir un espacio digital seguro.

En otras palabras, la UIT ha diseñado instrumentos técnicos para abordar los retos de la era digital, que representan una problemática interestatal que requiere amplios esfuerzos de articulación y cooperación. Bajo esas ideas, este trabajo entiende que Ecuador y Colombia -Estados- no pueden construir un ciberespacio seguro unilateralmente; por lo que, concurren a la UIT para asumir una agenda común, que de materializarse genera amplios beneficios para su desarrollo socioeconómico.

3) Marco conceptual

3.1. Unión Internacional de Telecomunicaciones UIT

La UIT constituye el organismo especializado de las Naciones Unidas para las TICs; por lo que, se encarga de regular las telecomunicaciones, a escala internacional. Nació en 1865 con el objetivo de normar la interconexión de los sistemas telegráficos internacionales. Conforme avanzó el desarrollo científico y tecnológico, esta institución evolucionó para asegurar las comunicaciones del mundo actual, ya en calidad de organismo especializado de la ONU. En las últimas décadas, la masificación de las TICs

amplió los campos de acción de este organismo, llegándosele a responsabilizar la construcción de un marco de cooperación para la seguridad digital.

Conforme los lineamientos establecidos en la CMSI (2003 – 2005), la UIT juega un rol importante en la generación de seguridad y confianza digital; ya que, es la institución responsable de implementar un marco de cooperación específico para esta materia. Por ende, en 2007, lanzó su Agenda Global para la Ciberseguridad, que promueve el trabajo técnico en dos niveles. En el nivel internacional, los esfuerzos de los actores estatales y no estatales deben centrarse en la articulación y cooperación técnica, buscando reducir los riesgos globales generados por la dependencia tecnológica. En el plano nacional, el Estado debe propiciar la implementación de una estrategia integral, que promueva la corresponsabilidad de todos los actores interesados; es decir, las instituciones públicas, el sector privado y las personas.

En el segundo nivel de trabajo, en 2018, la UIT facilitó la Guía -referida en líneas anteriores-, un instrumento construido con diferentes actores nacionales e internacionales, públicos y privados (UIT, 2022). Con el propósito de suministrar un conjunto de principios y ejes de trabajo comunes, que guíen el proceso de adopción de estrategias nacionales de seguridad cibernética (UIT, 2022). De esto último, surge el interés por indagar sobre la influencia que este documento técnico ha tenido en el desarrollo de políticas de ciberseguridad en dos Estados -Colombia y Ecuador-, durante el periodo 2018 – 2021.

3.2. Ciberseguridad

El concepto de ciberseguridad es contemporáneo, nació en el ámbito internacional para introducir el tema de la seguridad de los elementos digitales -incluso los físicos- en la agenda global (Ospina y Sanabria, 2020). Puesto que, el desarrollo de

las TICs supuso el crecimiento exponencial de las ciberamenazas y, con ello, los actores internacionales -organismos y Estados, principalmente- propiciaron espacios de debate, tales como la CMSI. Por su parte, los Estados entendieron a la seguridad cibernética como el conjunto de políticas, estrategias y normas, formuladas e implementadas para proteger la integridad de los activos físicos y digitales y, para prevenir, sancionar y mitigar los delitos informáticos (O'Connell, 2012).

Sobre el concepto, la UIT (2018) entiende la ciberseguridad como el conjunto de instrumentos, de carácter normativo, técnico y tecnológico, que un Estado, una organización o un ciudadano emplea para proteger sus activos digitales conectados a la red. Puesto que, la construcción de seguridad cibernética requiere el uso de diferentes herramientas, tales como políticas públicas, leyes, modelos de gestión, buenas prácticas internacionales e incluso tecnologías innovadoras (UIT, 2018). Todas ellas diseñadas para asegurar la integridad de los datos contenidos en la web y la seguridad física de las infraestructuras que permiten el funcionamiento de las TICs.

Desde una visión estatal, la ciberseguridad es el conjunto de capacidades desarrolladas por el Estado para reducir las amenazas a las que están expuestas sus infraestructuras esenciales -físicas y digitales- y los activos de los actores privados y las personas (CONPES, 2020). De manera que, el propósito de la seguridad digital es precautelar la integridad de los datos, las telecomunicaciones, los servicios electrónicos, los dispositivos vinculados a Internet y todas las infraestructuras estratégicas para el funcionamiento público (UIT, 2018).

Con el objeto de establecer los límites de la ciberseguridad, es importante definir ciberdefensa. Desde una visión de defensa nacional, la ciberdefensa es el conjunto de acciones preventivas, activas y reactivas que utilizan las fuerzas militares para gestionar

los ataques cibernéticos, que vulneran la independencia, la integridad territorial, la soberanía nacional, el orden jurídico interno y los intereses estatales (CONPES, 2016).

En otras palabras, la ciberdefensa es el conjunto de políticas y recursos, de origen militar, que se utiliza para garantizar la independencia y soberanía nacional en el espacio cibernético. Mientras que, la ciberseguridad es aquel conjunto de políticas, estrategias, acciones y recursos que posee el Estado para prevenir, combatir y sancionar el cibercrimen, es decir, aquellas actividades ilegales que se cometen mediante el empleo de las TICs y tienen por víctima principal a las personas (CONPES, 2016).

Para la ciberdefensa, las amenazas cibernéticas son dos. Primero, el ciberespionaje es una práctica ilegal para recabar información almacenada en el espacio cibernético, sin el consentimiento del titular; a fin de adquirir ventajas competitivas, de carácter económico, político, social e incluso militar. Segundo, el ciberterrorismo es el mal uso de los activos digitales para vulnerar los derechos humanos u ocasionar miedo en la población (CONPES, 2016). Por su parte, la ciberseguridad concibe a la ciberdelincuencia como su principal amenaza, misma que se entiende como aquellas actividades ilegales cometidas mediante la utilización de las TICs; con el propósito de obtener beneficios propios -generalmente económicos o políticos- y/o desestabilizar el Estado (CONPES, 2020).

Bajo esas ideas, esta investigación únicamente revisa la ciberseguridad; ya que, la política pública estudiada corresponde al enfoque de seguridad nacional, que tanto en Colombia como en Ecuador promueve -en lo principal- la protección de los derechos de las personas. Es decir, el análisis se concentra en las políticas públicas implementadas para gestionar y mitigar los ciberriesgos, que atentan contra la integridad de los ciudadanos y las entidades -públicas o privadas- que proporcionan bienes y/o servicios fundamentales para el desarrollo nacional.

3.3. Políticas Públicas

Entendida como objeto de estudio, la política pública es el conjunto de estrategias que se pueden atribuir a una autoridad, en el ejercicio cotidiano de sus funciones, ante las diversas problemáticas coyunturales que enfrenta. Dichas estrategias se consideran públicas cuando sirven a los intereses colectivos y, además, responden al conjunto de las voluntades comunes integradas por las propias de cada ciudadano (Bazúa y Valenti, 1995).

A decir de Thoenig (1997), la política pública resulta de las actividades desarrolladas por una autoridad legítima para solventar una problemática determinada. Esto es, el resultado del trabajo cotidiano que se desarrolla en diferentes fases, que incluyen la identificación de los problemas públicos y su priorización, la definición de líneas y estrategias de acción, la toma de decisiones, la implementación y, la evaluación (Thoenig, 1997).

En ese sentido, la política pública se integra por las estrategias adoptadas por una autoridad, durante el ejercicio de sus funciones. Si bien se entiende el origen de las políticas públicas, es necesario recurrir al concepto de Roth (2002) para comprender que todo trabajo público tiene por objetivo central incidir en la sociedad. En ese sentido, este autor define a la política pública como el conjunto de objetivos colectivos que son revisados, al menos de forma parcial, por una entidad gubernamental; con el objetivo de guiar el comportamiento de los actores -individuos y grupos- para cambiar una situación problemática (Roth, 2002).

Con esos antecedentes, el presente trabajo analiza la influencia que la Guía, un documento de origen internacional, ha tenido en la adopción de políticas de seguridad digital en Colombia y Ecuador, entre los años 2018 y 2021. Para ello, se entiende que

los riesgos y las amenazas cibernéticas suponen un problema común a todos los Estados; ya que, al vivir en una aldea global, las consecuencias negativas del mal uso y abuso de las TICs afectan a todos los países, a sus instituciones y ciudadanos. De ahí, surge la necesidad de que los organismos internacionales orienten el accionar estatal, mediante el establecimiento de agendas comunes que al ser asumidas y ejecutadas generan beneficios domésticos.

4) Metodología

El presente trabajo es cualitativo, de carácter descriptivo; ya que, indaga sobre la influencia de la Guía en la implementación de políticas de ciberseguridad en Colombia y Ecuador, entre 2018 y 2021, partiendo de la definición de aspectos concordantes entre el instrumento técnico de la UIT y las políticas nacionales de Colombia y Ecuador. Bajo el propósito de analizar la relación interdependiente que existe entre la Guía de la UIT y los instrumentos domésticos colombianos y ecuatorianos.

A decir de Ortiz (2015), la metodología descriptiva permite identificar las características de un objeto de estudio para definir la relación que existe entre las variables y, consecuentemente, obtener una conclusión. En ese sentido, esta investigación pretende explicar la relación existente entre una institución internacional y el comportamiento de dos Estados; a fin de determinar si la UIT incidió en las políticas nacionales de ciberseguridad de Colombia y Ecuador.

En la investigación, se utilizan fuentes de información primarias y secundarias. Las fuentes primarias son los documentos emitidos oficialmente por la UIT y por las instancias públicas competentes de Colombia y Ecuador. Por su parte, las fuentes secundarias son artículos académicos, obtenidos de bibliotecas virtuales especializadas en estudios de las Ciencias Sociales. Para sistematizar la información se recurre a

matrices que permitan efectuar un estudio comparado de los instrumentos adoptados por la UIT y los dos países en cuestión y, de esa manera, definir los ejes de trabajo domésticos en los que la institución internacional ha influenciado.

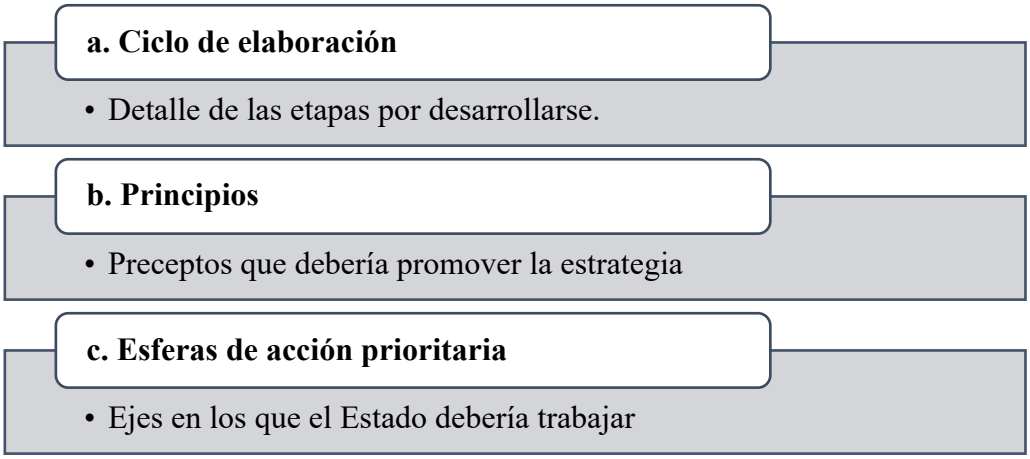
5) Resultados

5.1. Sobre la Guía de la UIT – versión 2018

En 2018, la UIT -juntamente con otras organizaciones internacionales como el Banco Mundial, la OTAN y Commonwealth- proporcionó la Guía; con la finalidad de encaminar los procesos de implementación de estrategias nacionales de seguridad digital. En dicho documento se presentan contenidos fundamentales para guiar a las autoridades nacionales, encargadas de formular, implementar, efectuar el seguimiento y evaluar los instrumentos nacionales. Todos estos insumos se presentan de manera ordenada y secuencial, conforme las secciones detalladas a continuación:

Ilustración 1:

Contenidos propuestos por la UIT en la Guía



Elaboración: Propia

Fuente: UIT, 2018

La Guía proporciona un marco de trabajo útil para las autoridades estatales inmersas en los procesos de diseño, ejecución, evaluación y reformulación de

estrategias de ciberseguridad, promoviendo así que cada Estado posea herramientas ajustadas a su realidad nacional, pero también armónicas con las propuestas y prácticas internacionales. Ya que, la UIT entiende que los asuntos de seguridad cibernética no son responsabilidad exclusiva de los Estados y, por ende, no pueden solventarse únicamente en el ámbito doméstico. Por el contrario, demandan acciones conjuntas y articuladas entre una diversidad de actores interesados, ya sean públicos o privados. Por ello, esta investigación utiliza el contenido de las secciones descritas para realizar el estudio comparado con el accionar doméstico de Colombia y Ecuador.

5.2. Política de ciberseguridad del Estado colombiano

Colombia adoptó su actual política de seguridad digital en 2020, a través del instrumento CONPES 3995, vigente hasta diciembre de 2022; con la finalidad de definir las estrategias de acción que permitan fortalecer la confianza digital y, paralelamente, mejorar la ciberseguridad nacional (CONPES, 2020). De tal manera que, Colombia se consolidaría como una sociedad integradora y competitiva en la era digital. Para lo consecución de dicho objetivo, se plantearon tres objetivos específicos: 1. Fortalecer las capacidades de todas las partes interesadas -Estado, sector productivo y personas-; 2. Fortalecer la institucionalidad de la ciberseguridad y, 3. Implementar modelos, estándares y buenas prácticas internacionales.

En la presente investigación, el objeto de estudio es el documento CONPES 3995; sin embargo, resulta importante entender que, desde 2011, Colombia ha desarrollado políticas públicas de seguridad cibernética secuenciales. Ya que, los resultados de las fases de monitoreo y evaluación han sido la base para potenciar, formular o reestructurar las estrategias de acción existentes. Bajo esa lógica, con el Documento 3701 de 2011, el Estado colombiano adoptó su primera política nacional de

ciberseguridad, buscando potenciar las capacidades públicas que le permitan reducir y gestionar los ciberriesgos y, subsiguientemente, construir un ciberespacio seguro para los colombianos (CONPES, 2011).

Sobre los resultados obtenidos, CONPES (2020) destaca el trabajo efectuado en materia institucional, especialmente en lo que se refiere a instituciones de gobernanza digital y creación de capacidades públicas. En cuanto a las instituciones, a partir de 2011, Colombia cuenta con tres instancias de coordinación y gestión de ciberamenazas, integradas por las entidades competentes de la Función Ejecutiva. Por otro lado, las capacidades estatales se desarrollaron gracias a los programas de capacitación que proporcionó el Grupo de Respuesta a Emergencias Cibernéticas de Colombia COLCERT (CONPES, 2016).

A pesar de estos avances, Colombia consideró que los esfuerzos nacionales no fueron suficientes; toda vez que, no incluyeron a todos los actores interesados, sino que se concentraron en los públicos. Por ello, CONPES (2016) resalta que la primera política pública fue limitada al momento de integrar a los representantes privados, los académicos y los ciudadanos en los procesos de fortalecimiento de capacidades digitales. Así también, el Estado colombiano reconoció la creciente necesidad de coordinar y articular acciones, nacionales e internacionales, una estrategia que no fue considerada ampliamente en su primera política de ciberseguridad (CONPES, 2016).

Tras la evaluación final del instrumento CONPES 3701, se adopta el Documento CONPES 3854 de 2016, la segunda política colombiana de ciberseguridad que promueve un enfoque de responsabilidad compartida. En otras palabras, la participación de todos los actores interesados es elevada a estrategia central para el fortalecimiento de las capacidades nacionales que permiten gestionar oportunamente los riesgos digitales (CONPES, 2016). Con ello, Colombia asumió que la construcción de un ciberespacio

seguro requiere de amplios niveles de participación de las entidades públicas y privadas, nacionales e internacionales y, esencialmente, de los ciudadanos colombianos.

En el marco de referida política, el Estado colombiano fortaleció su institucionalidad desde una visión de prevención de riesgos, que propone actuar antes de la materialización de los ciberataques y no solo reaccionar frente a ellos (CONPES, 2020). Entre las iniciativas de carácter preventivo, destacan los proyectos de sensibilización y de desarrollo de capacidades digitales ciudadanas, impulsados principalmente por el Ministerio de Ministerio de Tecnologías de la Información y las Comunicaciones -en adelante MINTIC- (CONPES, 2020). Así, esta Institución, juntamente con la Organización de Estados Americanos OEA, ejecutó dos proyectos educativos con enfoque de género, denominados *Por TIC Mujer* y *Hacker Girls*; con el objeto de crear capacidades digitales que permitan empoderar a las niñas, adolescentes y mujeres en la utilización de las TICs.

Si bien Colombia implementó iniciativas para la creación de capacidades nacionales, no logró involucrar a todos los actores interesados. Puesto que, los programas de capacitación y profesionalización nuevamente tuvieron como destinatarios principales a los servidores públicos de los sectores de las telecomunicaciones, la seguridad pública y la defensa nacional (CONPES, 2020). En otras palabras, la segunda política de ciberseguridad tampoco logró la participación de las instituciones privadas, la academia y las personas. Frente a ello, en 2020, el Estado colombiano adoptó su tercera política de ciberseguridad, mediante el Documento CONPES 3995, que busca superar la problemática de la baja participación de los actores no estatales.

En ese orden de ideas, entre 2011 y 2021, el Estado colombiano implementó tres políticas de seguridad digital que buscaron fortalecer las acciones exitosas y, a su vez,

plantear nuevas estrategias que se ajusten a los modernos retos digitales. En lo principal, Colombia desarrolló instrumentos públicos que le permitan involucrar a los diversos sectores interesados; ya que, las autoridades nacionales entendieron que no se puede construir un esquema nacional de ciberseguridad de manera aislada y unilateral.

Si bien se revisó brevemente los objetivos y avances de las dos primeras políticas de ciberseguridad de Colombia, el análisis comparado se concentra en los planteamientos efectuados en la tercera política nacional, contenida en el instrumento CONPES 3995; toda vez que, este documento se emitió en los años en estudio.

5.3. Política de ciberseguridad del Estado ecuatoriano

La política pública de ciberseguridad ecuatoriana es mucho más reciente que la colombiana; puesto que, Ecuador adoptó su primera política de seguridad digital en mayo de 2021. Como objetivo principal, el Estado propuso definir las líneas de acción que deberían observar todos los sectores interesados en la seguridad digital (MINTEL, 2021). Puesto que, antes de este instrumento, los esfuerzos fueron variados, poco coordinados, dispersos e incluso desarticulados. A pesar de ello, cabe revisar los avances obtenidos desde 2011, año en el que se introduce el tema de la seguridad cibernética en la agenda nacional. Así, el programa Ecuador Digital Versión 2.0 de 2011 encargó a las instituciones públicas el desarrollo de actividades tendientes a potencializar el uso de las TICs para el desarrollo nacional, en el marco de un ciberespacio seguro (MINTEL, 2021).

En 2013, las instituciones de la Función Ejecutiva implementaron un esquema de seguridad de la información, que constituye un marco útil para la gestión de los riesgos que atentan contra la integridad de la información que reposa en las bases de datos del sector público (MNTEL, 2021). Tras la fase de evaluación, el MINTEL

actualizó dicho esquema, promoviendo esta vez un modelo de gestión de mejora continua que deberían adoptar todas las entidades estatales; con la finalidad de contar con instrumentos que evolucionen conforme los retos digitales (Gobierno Electrónico, 2022).

Con el objeto de proporcionar asistencia técnica en los procesos de prevención y gestión de los ataques cibernéticos perpetrados contra las instituciones públicas del sector de telecomunicaciones y los prestadores de estos servicios, Ecuador estableció un centro de respuesta a incidentes informáticos nacional, adscrito a la Agencia de Regulación y Control de Telecomunicaciones ARCOTEL (MINTEL, 2021). Sobre sus funciones, MINTEL (2021) observa que dicho centro actúa de forma limitada; toda vez que sus actividades deben responder exclusivamente a lo determinado en la Ley Orgánica de Telecomunicaciones. A pesar de que, la Institución tiene la facultad de asistir a todas las instituciones públicas y privadas que demanden sus servicios (MINTEL, 2021).

Con la publicación del Plan de Gobierno Electrónico -versión 2016-, Ecuador promovió un modelo estándar de seguridad digital para las instituciones que integran y dependen de la Función Ejecutiva, buscando potencializar las capacidades estatales que permiten manejar los sistemas informáticos de manera eficiente y eficaz (MINTEL, 2021). En 2018, a través de una norma técnica, la ARCOTEL proporcionó una lista de incidentes cibernéticos comunes; así como, sus respectivos protocolos de acción.

En 2019, el Estado ecuatoriano adopta su Política Ecuador Digital, en la que instituye que la ciberseguridad es un eje de trabajo fundamental para el desarrollo nacional; ya que, las interacciones socioeconómicas cada vez más se desarrollan por medios digitales. A partir de ello, MINTEL implementó varios proyectos tendientes a cerrar la brecha digital y, consecuentemente, a garantizar el acceso a los servicios

públicos digitales (MINTEL, 2021). Todo ello desde un enfoque de máxima protección de los derechos de las personas.

Aunque Ecuador ha trabajado en materia de ciberseguridad desde 2011, recién en 2021 adoptó una política pública que integra las estrategias descritas anteriormente; a fin de, proporcionar un marco de acción único, que responda a los intereses nacionales. Dicho instrumento es objeto de análisis de la presente investigación; ya que, fue implementado por el Estado ecuatoriano durante el periodo en análisis (2018 – 2021).

5.4. Estudio comparado entre la Guía de la UIT y las políticas de seguridad digital de Colombia y Ecuador, adoptadas entre 2018 y 2021

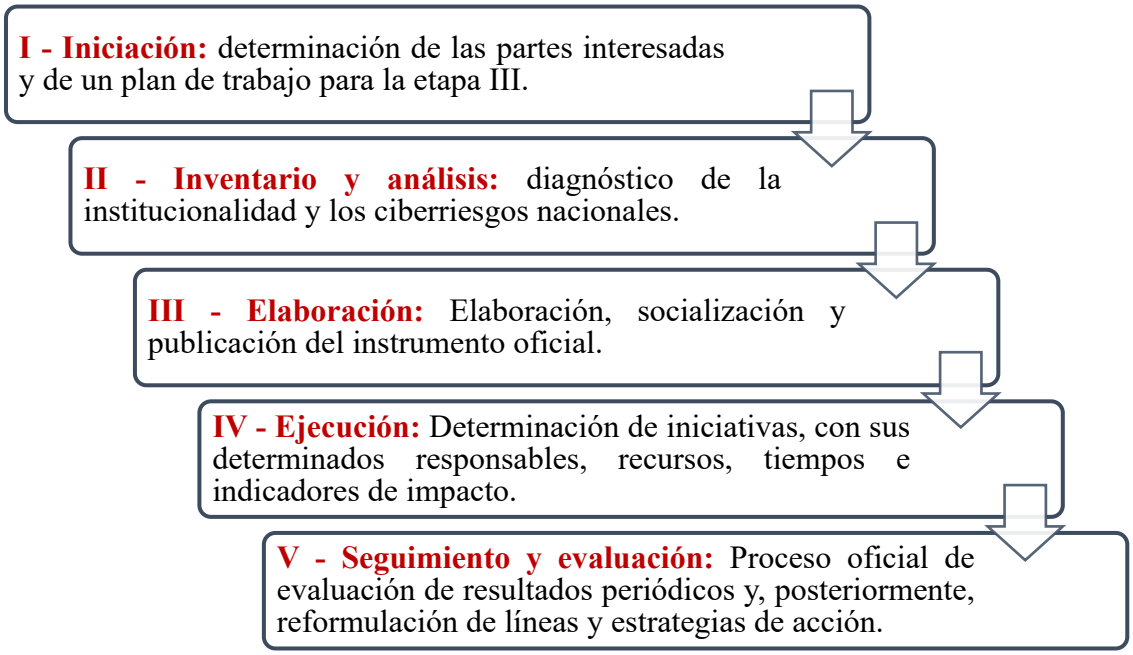
En esta sección, los contenidos propuestos en la Guía de la UIT se comparan con los planteamientos nacionales del Estado colombiano y el Estado ecuatoriano; con la finalidad de analizar la incidencia de esta institución internacional en sus asuntos domésticos. De manera que, se pueda identificar la existencia de una relación de interdependencia entre estos actores del sistema internacional. Para los fines consiguientes, se contrastan tres aspectos específicos: a. ciclo de vida de la estrategia, b. principios rectores y, c. esferas de acción prioritaria.

a. Ciclo de vida propuesto por la UIT en la Guía

En la Guía, la UIT propone un ciclo para la elaboración de las políticas nacionales de seguridad cibernética; a fin de que las autoridades nacionales desarrollen un proceso ordenado y sistemático, cuyo resultado sea un instrumento fundamentado en el contexto nacional, pero concordante con las prácticas internacionales. En ese sentido, la ilustración subsiguiente expone las fases planteadas:

Ilustración 2:

Ciclo de vida propuesto por la UIT en la Guía (2018)



Elaboración: Propia

Fuente: UIT, 2018

En cada etapa, la UIT propone varias acciones que deberían efectuarse para contar con un instrumento estatal adecuado, que en lo principal promueva una visión nacional única de ciberseguridad. La tabla No. 1 presenta dichas fases y sus elementos esenciales, de manera comparativa con las políticas nacionales de Colombia y Ecuador.

Tabla 1:

Cuadro comparativo entre el ciclo de vida planteado por la UIT en la Guía (2018) y las políticas nacionales implementadas por Colombia y Ecuador, entre 2018 y 2021

Guía de la UIT		**Colombia**	**Ecuador**
Ciclo de vida			
Fase I: Iniciación	Definición de la autoridad responsable	X	X
	Determinación del Comité Directivo	X	X

	Identificación de las partes involucradas	X	X
	Planificación de la elaboración del instrumento	-	X
Fase II: Inventario y análisis	Diagnóstico del panorama de ciberseguridad	X	X
	Diagnóstico de los ciberriesgos	-	X
Fase III: Elaboración	Elaboración	X	X
	Consulta a los actores interesados	-	X
	Aprobación oficial	X	X
	Publicación	X	X
Fase IV: Ejecución	Diseño del plan de acción	X	X
	Definición de iniciativas	X	X
	Determinación de recursos -humanos y financieros-	X	-
	Definición de cronogramas e indicadores de impacto	X	X
Fase V: Seguimiento y evaluación	Definición del proceso de evaluación	-	-
	Supervisión periódica de resultados	X	X
	Evaluación final de los resultados	X	-

Elaboración: Propia

En la primera fase, el instrumento ecuatoriano proporciona información detallada sobre cada uno de los elementos propuestos por la UIT; mientras que, Colombia describe tres de ellos. En Ecuador, se responsabiliza a MINTEL la elaboración de la política nacional y el liderazgo del Grupo Interinstitucional de Ciberseguridad, que fue la instancia de debate y coordinación de los asuntos de ciberseguridad hasta mayo de 2021 (MINTEL, 2021). Mientras que, el Estado colombiano instituye que el Consejo Nacional de Política Económica y Social -en adelante CONPES- tiene ambos roles; es decir, autoridad competente y comité directivo

del proceso de implementación de la estrategia nacional. Puesto que, este Consejo es el responsable de adoptar las políticas públicas necesarias para el desarrollo socioeconómico del país (Departamento Nacional de Planeación, 2022).

En la misma etapa, Colombia y Ecuador implementaron un enfoque de corresponsabilidad, que permite integrar a los múltiples actores interesados en cada una de las fases del ciclo de vida de las políticas nacionales. En otras palabras, ambos Estados consideraron trascendental la participación de las entidades estatales, el sector privado, los académicos y la ciudadanía. Por otra parte, Ecuador presentó una hoja de ruta para el diseño, socialización, publicación e implementación de su política nacional; mientras que, Colombia no informa sobre las acciones que se efectuaron antes de la publicación oficial de su instrumento.

Sobre la segunda fase, el Estado colombiano realiza una evaluación de los avances logrados a partir de su primera política de ciberseguridad, adoptada en 2011 y, paralelamente, determina las principales debilidades nacionales. Entre ellas, resalta el bajo nivel de participación de los actores no estatales; debido a que la mayoría de las iniciativas de fortalecimiento de capacidades tuvieron por destinatario a los funcionarios públicos (CONPES, 2020). Asimismo, Ecuador efectúa un estudio detallado de la estructura institucional existente y de los ciberriesgos que amenazan la seguridad pública; bajo el propósito de contar con un panorama completo de las fortalezas y debilidades nacionales.

En la tercera fase, la política ecuatoriana proporciona información sobre cada una de las propuestas de la UIT; mientras que, el instrumento colombiano se refiere a tres elementos. Sobre la visión nacional clara, ninguna de las políticas presenta una perspectiva estatal única; sin embargo, se cuenta con objetivos concretos. Por su parte, la estrategia colombiana busca generar confianza digital para potenciar el desarrollo de

las interacciones socioeconómicas digitales. Mientras que, el Estado ecuatoriano propone potenciar las capacidades nacionales y, de esa manera, asegurar el ejercicio de derechos y libertades.

Así también, la estrategia colombiana vigente resulta de la evaluación de sus dos políticas de ciberseguridad anteriores, mas no del debate con actores no estatales interesados. En tanto que, la política ecuatoriana es más integradora, ya que el documento borrador fue socializado telemáticamente con la ciudadanía, mediante la plataforma Diálogo 2.0 (MINTEL, 2021).

Adicionalmente, la UIT sugiere que la estrategia nacional se adopte como política pública o ley. En ambos casos, las estrategias se implementaron como políticas públicas, pero de diferente origen. Puesto que, nacen en instancias distintas. Así, el instrumento colombiano se construye en un órgano colegiado de debate y coordinación de asuntos socioeconómicos; mientras que, el documento ecuatoriano es elaborado y publicado por MINTEL, mediante Acuerdo Ministerial No. 006-2021 de mayo de 2021.

En la cuarta etapa, el Estado colombiano formula un plan de acción concreto, con iniciativas, recursos humanos y económicos, temporalidades y, mecanismos de monitoreo y evaluación específicos. Es decir, se cuenta con un panorama de acción claro. En contraste, la política ecuatoriana no determina tiempos de ejecución ni recursos necesarios, a pesar de presentar diversas iniciativas con sus respectivos responsables e indicadores de impacto. En ese sentido, esta última política nacional es susceptible de materializarse conforme el compromiso y los recursos que posea cada entidad responsable, pudiéndose afectar así las fases de ejecución y evaluación.

En la fase de seguimiento y evaluación, el Estado colombiano plantea un procedimiento de monitoreo periódico y evaluación general; a fin de que, los alcances obtenidos sean evaluados oportunamente. De modo que, las estrategias exitosas sean

fortalecidas y, a su vez, los nuevos desafíos se afronten preventivamente, sobre la base de la creación de capacidades nacionales. Como responsable de esta etapa, el Departamento Nacional de Planeación debe presentar el informe final el 31 de diciembre de 2022, documento que constituirá el punto de partida de la nueva estrategia nacional. En el caso ecuatoriano, la política de ciberseguridad no determina una entidad responsable de esta etapa, ni tampoco plazos de ejecución de cada iniciativa. Empero, sí se especifica su vigencia hasta el año 2023.

b. Principios propuestos por la UIT en la Guía (2018)

En la Guía, la UIT propone a las autoridades públicas nacionales trabajar sobre la base de nueve principios generales, que deberán priorizarse conforme los intereses nacionales de cada país. De manera que, las líneas de acción estratégica propuestas se materialicen oportunamente, propiciando así la creación de un ciberespacio seguro para el desarrollo de las interacciones socioeconómicas. En ese sentido, la tabla No. 2 presenta los principios que Colombia y Ecuador han promovido en sus estrategias nacionales.

Tabla 2:

Cuadro comparativo entre los principios propuestos por la UIT en la Guía (2018) y las políticas nacionales implementadas por Colombia y Ecuador, entre 2018 y 2021.

Guía de la UIT **Principios**	**Colombia**	**Ecuador**
Visión nacional clara	-	-
Análisis integral y prioridades nacionales	X	X
Inclusividad	X	X
Desarrollo socioeconómico	X	X
Derechos humanos	X	X
Gestión de riesgos y resiliencia	X	X

Instrumentos políticos adecuados	-	-
Institucionalidad clara y recursos definidos	X	-
Entorno de confianza digital	X	X

Elaboración: Propia

Ambos Estados han adoptado parte de los principios propuestos por la UIT; ya que, reconocen que el trabajo en ciberseguridad debe articularse con los intereses nacionales y los objetivos de las agendas globales. En ese sentido, Colombia asimiló siete de los nueve preceptos y, Ecuador adoptó seis de ellos. En el caso colombiano, las iniciativas adoptadas se enmarcan en:

a. Análisis integral y prioridades nacionales: El CONPES No. 3995 presenta un diagnóstico completo de las capacidades estatales y la estructura institucional existente; así como, de los retos que enfrenta el Estado colombiano; con la finalidad de ajustar las líneas de acción estratégica al contexto nacional. En ese sentido, se propone trabajar en la generación de capacidades digitales que aseguren el desarrollo de relaciones socioeconómicas en el espacio cibernético.
b. Inclusividad: La estrategia nacional concibe la corresponsabilidad como uno de sus enfoques fundamentales, al reconocer que la adopción de esquemas de ciberseguridad demanda la participación de todas las instituciones estatales, los actores privados y las personas y, paralelamente, requiere el fortalecimiento de la cooperación bilateral y multilateral.
c. Desarrollo socioeconómico: La política instituye que la ciberseguridad es un eje de trabajo trascendental para el desarrollo nacional; por lo que, las iniciativas propuestas buscan generar capacidades nacionales y fomentar la investigación en TICs para el desarrollo.

d. Derechos humanos: El Estado colombiano promueve la generación de capacidades ciudadanas para asegurar que los derechos fundamentales no sean vulnerados, durante la utilización de las TICs. Asimismo, las iniciativas presentan especial interés en la mujer, buscando empoderarla a través del desarrollo de habilidades digitales y, de esa manera, reducir la desigualdad de género.
e. Gestión de riesgos y resiliencia: En la política de ciberseguridad de 2016, Colombia implementó un enfoque preventivo, que se fortalece con la estrategia de 2020, mediante el desarrollo de programas de formación digital para los servidores públicos. Entre los contenidos impartidos, CONPES (2020) resalta las buenas prácticas internacionales en el ámbito de la educación para la prevención.
f. Institucionalidad y recursos: Desde 2011, Colombia cuenta con una estructura institucional especializada en el desarrollo de política pública y estrategias de gestión de riesgos cibernéticos; así como, con recursos financieros específicos para financiar las iniciativas nacionales. Dentro de la institucionalidad resalta el CONPES como máxima instancia de adopción de las estrategias nacionales y, los centros de respuesta a incidentes de los sectores de la defensa y seguridad (CONPES, 2020).
g. Entorno de confianza digital: La política de ciberseguridad establece que la confianza digital es una condición trascendental para el desarrollo nacional; ya que, solo un entorno seguro propicia el desarrollo de interacciones socioeconómicas a gran escala. De ahí que, Colombia invierta en proyectos de generación de capacidades cibernéticas, dirigidos a todas las partes interesadas.

En el caso ecuatoriano, la política de ciberseguridad adopta seis de los nueve principios de la UIT, de acuerdo con el siguiente detalle:

a. Análisis integral y prioridades nacionales: La estrategia nacional revisa los esfuerzos efectuados desde 2011 -año en que se introduce el tema de ciberseguridad en la agenda nacional- y, a su vez, caracteriza los incidentes cibernéticos más comunes en el país. A partir de ello, la generación de capacidades nacionales se eleva a eje fundamental para el desarrollo económico y social del país.
b. Inclusividad: En la misma línea que Colombia, el Estado ecuatoriano promueve la corresponsabilidad como elemento esencial en la construcción de esquemas de seguridad digital. De manera que, se instituye que las contrapartes esenciales son los actores no estatales, ya sean de origen nacional o internacional.
c. Desarrollo socioeconómico: Al igual que la política colombiana, el instrumento ecuatoriano reconoce el potencial de las TICs para el desarrollo económico y social; por lo que, se propone implementar marcos de acción que permitan masificar las interacciones digitales seguras.
d. Derechos humanos: Para Ecuador, la protección de los derechos humanos y el pleno ejercicio de las libertades fundamentales, en el ámbito digital, son prioridades nacionales; por lo que, desde los ministerios rectores de telecomunicaciones y educación se desarrollan proyectos de formación de ciudadanos digitales, es decir, de sujetos de derechos y obligaciones.
e. Gestión de riesgos y resiliencia: En su segundo pilar, la estrategia nacional establece que la protección de los activos digitales -especialmente los datos personales- es una prioridad nacional; toda vez que, la funcionalidad del Estado y la sociedad misma requiere contar con marcos de acción estandarizados, que permitan minimizar las consecuencias e incluso reducir la incidencia de los ciberataques.

f. Entorno de confianza digital: Al igual que Colombia, Ecuador concibe la generación de confianza digital como elemento esencial para la masificación de las interacciones socioeconómicas digitales; por lo que, dentro del pilar siete, la estrategia nacional propone trabajar en la creación de capacidades nacionales a través de la profesionalización y la sensibilización.

En ese orden, Colombia y Ecuador adoptaron parte de los principios propuestos por la Institución Internacional, articulando así sus intereses nacionales con los planteamientos de la agenda global de seguridad digital de la UIT. Es decir, se corrobora que los Estados no pueden implementar estrategias nacionales de manera aislada, considerando únicamente las necesidades domésticas; por el contrario, deben fomentar el desarrollo de marcos de acción armónicos, que les permita cooperar con otros actores, en todos los niveles -local, nacional, regional y global-.

c. Esferas de trabajo propuestas por la UIT en la Guía (2018)

La UIT plantea siete esferas de trabajo, en las que los responsables de implementar la estrategia nacional deberían proponer acciones específicas, que se ajusten al contexto de cada país y conforme los intereses nacionales. En otras palabras, el Estado priorizará sus actuaciones en uno u otro eje con base en el análisis de la estructura institucional, los riesgos y amenazas cibernéticas y, las demandas ciudadanas. A continuación, la tabla No. 3 presenta las esferas de trabajo en las que Colombia y Ecuador han formulado programas o proyectos.

Tabla 3:

Cuadro comparativo entre las esferas de trabajo planteadas por la UIT en la Guía (2018) y las políticas nacionales adoptadas por Colombia y Ecuador, entre 2018 y 2021.

Guía de la UIT **Esferas de trabajo**	**Colombia**	**Ecuador**
Gobernanza	X	X
Gestión de riesgos	X	X
Preparación y resiliencia	X	X
Infraestructuras críticas y servicios fundamentales	X	X
Capacidades digitales	X	X
Legislación y reglamentación	X	X
Cooperación internacional	X	X

Elaboración: Propia

Colombia y Ecuador formularon actividades en cada uno de los ejes de trabajo propuesto por la UIT; empero, sus políticas nacionales se han centrado en un área específica. Así, el Estado colombiano tiene por principal interés la creación de capacidades digitales (eje de acción No. 5), en todos los sectores interesados -Estado, empresas y personas-. De ahí que, se hayan planteado 19 iniciativas de carácter educativo, con las cuales se pretende sensibilizar sobre los riesgos digitales y, paralelamente, construir habilidades para el uso productivo de las TICs. Dentro de dichas acciones, Colombia cuenta con proyectos emblemáticos que permiten entender que la política pública se materializa en territorio mediante acciones concretas.

Así, la iniciativa nacional Por TIC Mujer constituye un proyecto emblemático en materia de generación de capacidades digitales, con enfoque de género. Su origen se encuentra en la segunda política de ciberseguridad colombiana; sin embargo, se fortalece con la estrategia vigente; ya que, en esta se encarga al Ministerio TIC el

robustecimiento de las iniciativas exitosas (CONPES, 2020). Referente al proyecto, el Estado propuso empoderar a las mujeres en la utilización de las TICs, otorgándoles así la oportunidad de contar con destrezas informáticas para prevenir ciberataques y, paralelamente, desarrollar actividades digitales productivas (MINTIC, 2022).

En cuanto al impacto, MINTIC (2022) destaca que, entre 2019 y 2020, el proyecto benefició a 1565 organizaciones sociales de mujeres y 23097 colombianas de 34 departamentos (MINTIC, 2022). Entre las beneficiarias cabe destacar 306 víctimas del conflicto armado y 44 mujeres con discapacidad, ya que, se demuestra el interés estatal por incluir a los sectores vulnerables. A pesar de que dicha estadística no muestra el alcance actual, sí refleja que los lineamientos generales de la política nacional colombiana se han concretado en proyectos específicos, gracias a la inversión de 648 millones de pesos (MINTIC, 2022).

Asimismo, Ecuador centró su interés en la generación de capacidades nacionales, es decir, en el eje de trabajo cinco de la UIT. En ese sentido, se han desarrollado proyectos educativos tendientes a sensibilizar a la ciudadanía y a fomentar el alfabetismo digital. Así, “El Mundo Virtual de Eugenia” es una iniciativa conjunta del Ministerio de Educación, Edutec y Cisco Webex Academy, desarrollada para fortalecer las destrezas digitales de los estudiantes de bachillerato, así como de sus familias y docentes (MINEDUC, 2022).

Para la ejecución del proyecto, el Estado ecuatoriano responsabilizó a MINEDUC el diseño de los insumos que permitan sensibilizar sobre el empleo productivo de las TICs y, la prevención de incidentes digitales. Por su parte, la Institución amplió el alcance del proyecto inicial mediante la adopción de un conjunto de herramientas didácticas dirigidas a los estudiantes de todos los niveles (MINEDUC, 2022). En cuanto al impacto, MINEDUC procuró incidir en toda la población

estudiantil de los niveles básico y bachillerato, para ello se integraron temas digitales al pensum de estudios. De esa manera, Ecuador ha invertido en la creación de capacidades digitales en los grupos vulnerables, es decir, niños, niñas y adolescentes.

6) Conclusiones

El uso masivo de las TICs genera importantes ventajas socioeconómicas, pero también innumerables amenazas digitales que atentan contra la seguridad internacional y nacional y, el desarrollo social y económico de las naciones. Frente a ello, las instituciones internacionales -por ejemplo, UIT- han promovido agendas globales, cuya base es la cooperación entre actores estatales y no estatales, a escala nacional, regional y global. Por su parte, en 2018, la UIT facilitó un instrumento técnico a las autoridades nacionales, con la finalidad de promover la adopción de marcos de acción armónicos, pero ajustados a los intereses de cada país.

Entre 2018 y 2021, Colombia y Ecuador adoptaron sus políticas de ciberseguridad, con el propósito de fortalecer las capacidades estatales para la gestión de ciberriesgos y la prevención de incidentes digitales. Dichos instrumentos presentan sinergias con los planteamientos de la UIT, en lo relativo al ciclo de vida de la estrategia, los principios generales y las esferas de trabajo. De forma que, la política doméstica de ambos países está articulada con los objetivos y metas de una agenda global para la seguridad digital.

Referente al ciclo de la estrategia nacional, ambos Estados desarrollan las cinco etapas propuestas en la Guía de la UIT, de manera sistemática y ordenada. Sin embargo, las fases se desarrollan con mayor prolijidad en el caso colombiano; puesto que, las partes involucradas, las temporalidades, los recursos y las metodologías son mucho más

claras y, por ende, muestran un mapa completo de la visión de ciberseguridad colombiana, entre los años 2020 y 2022.

Asimismo, ambas políticas nacionales promueven parte de los principios planteados por la UIT, pero los adoptan en menor o mayor medida, según las prioridades e intereses nacionales. En Colombia, la política de ciberseguridad se concentra en fomentar la inclusividad; puesto que, se concibe la corresponsabilidad de los actores estatales como un elemento indispensable para construir capacidades estatales. Por su parte, Ecuador centra sus esfuerzos en la protección de los derechos humanos, mediante la creación de capacidades digitales en las partes interesadas, especialmente en la ciudadanía.

Igualmente, ambos Estados propusieron iniciativas en el marco de cada esfera de trabajo planteada por la UIT, concentrando mayores esfuerzos en aquellas prioritarias para cada uno. Colombia, por su parte, centra su atención en la generación de capacidades digitales, a través de la implementación de 19 actividades estratégicas de profesionalización y sensibilización, todas ellas bajo un enfoque de género, corresponsabilidad y protección de derechos. Del mismo modo, Ecuador concentra sus esfuerzos en la creación de capacidades cibernéticas, pero con especial interés en los niños, niñas y adolescentes.

Finalmente, la UIT influyó en la política doméstica de ciberseguridad de Colombia y Ecuador, desarrollada entre 2018 y 2021, mediante un instrumento técnico que proporciona información sobre las fases, los principios y ejes de trabajo de las políticas nacionales. Es decir, la Institución Internacional incidió en el accionar estatal de ambos países, que adoptaron parte de los objetivos de la agenda internacional de ciberseguridad. De modo que, se corrobora la existencia de una relación de

interdependencia entre la UIT y ambos Estados, cuyo resultado son estrategias nacionales armónicas con los postulados técnicos de una organización internacional.

7) Referencias

ARCOTEL. (2022). Centro de Respuesta a Incidentes Informáticos del Ecuador. Recuperado de: https://www.ecucert.gob.ec/centro-de-respuesta-a-incidentes-informaticos-del-ecuador/

Bazúa, F. y Valenti, G. (1995). ¿Qué es política pública? En Políticas Públicas y desarrollo municipal, pp. 51 – 82. Recuperado de: http://dgece.sev.gob.mx/docs/Bazua_y_Valenti_U-I_CL3.pdf

CONPES. (2011). CONPES 3701 Lineamientos de Política para Ciberseguridad y Ciberdefensa. Recuperado de: http://www.dnp.gov.co/CONPES/documentos-conpes/Paginas/documentos-conpes.aspx#Default={%22k%22:%22ConpesNumero:3701%20OR%20Title:3701%22}

CONPES. (2016). CONPES 3854 Política Nacional de Seguridad Digital. Recuperado de: https://www.dnp.gov.co/CONPES/documentos-conpes/Paginas/documentos-conpes.aspx#Default=%7B%22k%22:%22ConpesNumero:3854%20OR%20Title:3854%22%7D

CONPES. (2020). CONPES 3995 Política Nacional de Confianza y Seguridad Digital. Recuperado de: https://www.dnp.gov.co/CONPES/documentos-conpes/Paginas/documentos-conpes.aspx#Default=%7B%22k%22:%22ConpesNumero:3995%20OR%20Title:3995%22%7D

Departamento Nacional de Planeación. (2022). El Consejo Nacional de Política Económica y Social CONPES. Recuperado de: https://www.dnp.gov.co/CONPES/Paginas/conpes.aspx

Gobierno Electrónico. (2022). Esquema Gubernamental de Seguridad de la Información EGSI. Recuperado de: https://www.gobiernoelectronico.gob.ec/egsi-v2/

Grieco, J. y Ikenberry, J. (2002). State Power and World Markets: The International Economy. New York: W. W. Norton & Company.

Keohane, R. (1993). Instituciones internacionales y poder estatal. Buenos Aires: Grupo Editor Latinoamericano.

Ministerio de Defensa Nacional, Comando General de Fuerzas Militares y Escuela Superior de Guerra. (2020). Estrategia Nacional de Cibersdefensa y Ciberseguridad -ECDCS- 2020 - 2030. Bogotá, Colombia. ISBN: 978-958-52545-5-8

MINEDUC. (2022). El Mundo Virtual de Eugenia. Recuperado de: https://recursos2.educacion.gob.ec/euinicio/

MINEDUC. (2022). MINEDUC y CISCO promueven curso de ciberseguridad. Recuperado de: https://educacion.gob.ec/mineduc-y-cisco-promueven-curso-de-cyberseguridad/

MINTEL. (2021). Política de Ciberseguridad. Quito – Ecuador, 17 de mayo de 2021. Recuperado de: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Acuerdo-No.-006-2021-Politica-de-Ciberseguridad.pdf

MINTIC. (2022). Apropiación de las tecnologías: Por TIC Mujer. Recuperado de: https://colombiatic.mintic.gov.co/679/w3-propertyvalue-188412.html

MINTIC. (2022). Iniciativa Por TIC Mujer. Recuperado de: https://www.mintic.gov.co/micrositios/porticmujer/809/w3-propertyvalue-412231.html

O'Connell, M. (2012). Ciberseguridad sin ciberguerra. Revista de Conflicto y Ley de Seguridad, 17 (2), pp. 187 - 209. Recuperado de: https://www.jstor.org/stable/26296226

Ortiz, A. (2015). Métodos descriptivos de investigación. En Enfoques y métodos de investigación en las ciencias sociales y humanas, pp. 31 – 90. ISBN 978-958-762-399-4

Ospina, M. y Sanabria, P. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. Reviste Criminalidad, 62 (2), 199 – 217. Recuperado de: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082020000200199

Roth, A. (2002). Políticas Públicas, Formulación, Implementación y Evaluación. Ediciones Aurora, Bogotá, Colombia. Recuperado de: https://polpublicas.files.wordpress.com/2016/08/roth_andre-politicas-publicas-libro-completo.pdf

Stein, A. (2008). Neoliberalismo Institucional. En Reus-Smit, C. y Snidal, D., T*he Oxford Handbook of Internacional Relations*, pp. 201 - 221. ISBN 978-0-19-921932-2

Thoenig, J. (1997). Política Pública y acción pública. En Gestión y Política Pública, 6 (2), pp. 19 – 37. Recuperado de: http://repositorio-digital.cide.edu/bitstream/handle/11651/3185/TJ_Vol.6_No.I_1sem.pdf?sequence=1

Unión Internacional de Telecomunicaciones (ITU). (2022). Ciberseguridad. Recuperado de 2022 https://www.itu.int/es/about/Pages/default.aspx

Unión Internacional de Telecomunicaciones (ITU). (2022). Estrategias nacionales. Recuperado de: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx

Unión Internacional de Telecomunicaciones (ITU). (2018). Guía para la Elaboración de una Estrategia Nacional de Ciberseguridad 2018. Recuperado de: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-S.pdf

Unión Internacional de Telecomunicaciones (ITU). (2010). Sobre la Unión Internacional de Telecomunicaciones UIT. Recuperado de: http://www.itu.int/net/itunews/issues/2010/09/20-es.aspx

WSIS. (2004). Plan de Acción de Ginebra. Recuperado de: https://www.itu.int/net/wsis/docs/geneva/official/poa-es.html