ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA TECNOLÓGICA

CENTRO DE POSGRADOS

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

MAESTRÍA EN GERENCIA DE SISTEMAS

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TITULO DE MAGISTER EN GERENCIA DE SISTEMAS

TEMA: "DEFINICIÓN DE LA LÍNEA BASE DE LA CIBERSEGURIDAD EN EL ECUADOR Y SU PROYECCIÓN PARA ESTABLECER UNA POLÍTICA NACIONAL DE CIBERSEGURIDAD"

AUTOR: RIVERA PASTRANO, LUIS OSWALDO

DIRECTOR: ING. RON EGAS, MARIO BERNABÉ MSC.

SANGOLQUÍ

2019

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

CERTIFICACIÓN

Certifico que el trabajo de titulación, ***"DEFINICIÓN DE LA LÍNEA BASE DE LA CIBERSEGURIDAD EN EL ECUADOR Y SU PROYECCIÓN PARA ESTABLECER UNA POLÍTICA NACIONAL DE CIBERSEGURIDAD"*** fue realizado por el señor ***Rivera Pastrano, Luis Oswaldo*** el mismo que ha sido revisado en su totalidad, analizado por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Sangolquí, 14 de junio de 2019

Firma:

.....

Ing. Mario Bernabé Ron Egas MSc.

C.C.: 1704229747

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

AUTORÍA DE RESPONSABILIDAD

Yo, ***Rivera Pastrano, Luis Oswaldo***, con cédula de ciudadanía No. 171743560-4, declaro que el contenido, ideas y criterios del trabajo de titulación "***Definición de la línea base de la Ciberseguridad en el Ecuador y su proyección para establecer una Política Nacional de Ciberseguridad***" es de mi autoría y responsabilidad, cumpliendo con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Consecuentemente el contenido de la investigación mencionada es veraz.

Sangolquí, 14 de junio de 2019

Firma

.....

Luis Oswaldo Rivera Pastrano

C.C.: 1717435604

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

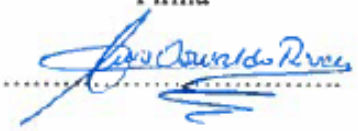
CENTRO DE POSGRADOS

AUTORIZACIÓN

Yo, ***Rivera Pastrano, Luis Oswaldo*** autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación ***"Definición de la línea base de la Ciberseguridad en el Ecuador y su proyección para establecer una Política Nacional de Ciberseguridad"*** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Sangolquí, 14 de junio de 2019

Firma



Luis Oswaldo Rivera Pastrano

C.C.: 1717435604

DEDICATORIA

A María Augusta y Miguel Antonio

Este trabajo está dedicado a ustedes, mi amada esposa y mi pequeño hijo. En ustedes he logrado ver el amor y la ternura, los cuales han servido de inspiración para continuar adelante, siempre tratando de ser un buen ejemplo en el hogar que estamos construyendo cada día. Su constante apoyo ha sido fundamental en la culminación de esta nueva meta. Va por ustedes.

A María Elena, Luis Oswaldo, Diego Mauricio y Cristina Gabriela

Sin los valores enseñados por ustedes, esto no sería posible. Me enseñaron que pesar de que tan dura es la situación, nunca se debe dejar de mirar el horizonte y se debe mantener la fe. Gracias a ustedes aprendí que la unión hace la fuerza. Este trabajo también se los dedico a ustedes.

Oswaldo

AGRADECIMIENTO

Al Ser Supremo, Padre de todos, el cual le agradezco por cada día de vida, por todo lo que me has dado, tus enseñanzas en cada día que pasa y han permitido alcanzar cada objetivo trazado. Gracias Padre.

A mi esposa y mi hijo, les agradezco mucho por ser el motor que me impulsa a ser mejor para ustedes. Compañera mía, cada muestra de amor y palabra de aliento fueron fundamentales para continuar y culminar con este reto, y cada sonrisa tuya mi querido hijo ha sido una inspiración para tratar de ser mejor, y ser tu guía por siempre.

A mis padres, cada enseñanza suya han sido pilares en muestra formación. Gracias por todo lo que me han sabido dar con mucho amor, han sido y serán mi ejemplo, les estaré siempre agradecidos. Mis hermanos, que han sido un gran apoyo en toda esta etapa, hoy que son cada vez mejores, han demostrado siempre humildad. Son excelentes profesionales y seres humanos.

A mis maestros, especialmente al Ing. Mario Ron, por la confianza depositada en mí, sus consejos, conocimientos y acertada tutoría, se logró que esta meta se culmine, y que servirá como base para futuros trabajos que beneficien al país.

Al Ministerio de Telecomunicaciones y de la Sociedad de la Información, a través de la Subsecretaría de la Sociedad de la Información y Gobierno en Línea, quienes me han ayudado con los insumos y las gestiones necesarias para desarrollar el presente proyecto, que servirá como base para continuar fomentando la Sociedad de la Información en el Ecuador.

A mi familia, amigos y compañeros, que con cada palabra de aliento han sabido impulsar el desarrollo de este trabajo.

A todos, por hacer posible esto, les agradezco en el alma.

Oswaldo

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Nuestro país carece de una Política o Estrategia Nacional que dicte lineamientos y acciones que permitan precautelar la seguridad en el Ciberespacio. Una de las causas a esta falencia es la falta de una línea base que muestre la situación actual del país en este aspecto, dejando con la incertidumbre de una situación actual a todos los actores gubernamentales, privados, académicos y sociedad civil, sobre las acciones que se deberían tomar ante amenazas, dejándolos expuestos y vulnerables a los usuarios de los servicios de las Tecnologías de la Información y Comunicación (TIC) en el ciberespacio. El presente trabajo de investigación muestra la situación actual de la Ciberseguridad en el Ecuador, formulada en base a la recopilación de información basada en una metodología de investigación aplicada y documental, pretendiendo tener una proyección hacia una Política o Estrategia Nacional en la que se incorporen lineamientos, acciones estratégicas y niveles de seguridad en el ciberespacio. La línea base de la Ciberseguridad se establece a través de los siguientes aspectos: Infraestructura de información, marco penal, sensibilización, capacitación y formación, cooperación nacional e internacional e institucionalidad, así podemos determinar la brecha que separa la realidad actual y la proyección de futuro. Este proyecto es muy importante para determinar en forma real y comprensible la situación del Ecuador referente a Ciberseguridad, además, establecer la brecha que tiene el Ecuador con otros países referentes, tanto en la región como en otros con un nivel de madurez más desarrollado.

PALABRAS CLAVE:

- **CIBERSEGURIDAD**
- **SEGURIDAD DE LA INFORMACIÓN**
- **LÍNEA BASE**

ABSTRACT

Our country lacks a National Policy or Strategy that dictates guidelines and actions that allow precautionary security in Cyberspace. One of the causes of this failure is the lack of a baseline that shows the current situation of the country in this aspect, leaving the uncertainty of a current situation to all government actors, private, academic and civil society, on the actions that they should be taken before threats, leaving them exposed and vulnerable to the users of the Information and Communication Technologies (ICT) services in cyberspace. The present research work shows the current situation of Cybersecurity in Ecuador, formulated based on the collection of information based on a methodology of applied research and documentary, pretending to have a projection towards a National Policy or Strategy in which guidelines are incorporated , strategic actions and levels of security in cyberspace. The baseline of Cybersecurity is established through the following aspects: Infrastructure information, criminal framework, awareness, training and cooperation, national and international cooperation and institutions, so we can determine the gap between current reality and future projection . This project is very important to determine in a real and understandable way the situation of Ecuador regarding Cybersecurity, in addition, to establish the gap that Ecuador has with other referring countries, both in the region and in others with a more developed level of maturity.

KEYWORDS:

- **CYBERSECURITY**
- **INFORMATION SECURITY**
- **BASELINE**

CAPÍTULO I. GENERALIDADES

1.1 Antecedentes

En la medida que la brecha digital disminuye en los países ante la necesidad de contar con el acceso de las tecnologías y con ellas a la información, así mismo, los riesgos a los que la ciudadanía se encuentra expuesta dentro del ciberespacio son cada vez más significativos, los ataques informáticos, robo de identidades y otras actividades son ejecutadas por personas o entidades que hacen mal uso de los sistemas de información, de manera más continua.

Los servicios y el avance tecnológico que conlleva la Industria 4.0 en la actualidad, se ven afectados por los ataques informáticos, entre ellos la banca, los servicios en la nube, los servicios de datos abiertos, Big Data, comercio electrónico, redes sociales y otros.

La línea base que permitirá más adelante generar políticas nacionales, debe considerar varios aspectos relacionados al estado técnico, jurídico, legal, cooperativo e institucional de la ciberseguridad; es necesario también analizar las acciones que organismos internacionales referentes a las TIC y la Seguridad de la Información han tomado con el fin de minimizar el impacto de los ataques informáticos, como los retos que la Agenda 2030 para Desarrollo Sostenible, aprobada en septiembre de 2015 por la Asamblea General de las Naciones Unidas ha considerado como amenazas en ciberseguridad, que incide en la capacidad de aprovechar las TIC e internet en los gobiernos, empresas y de los individuos. (UIT, 2015)

El robo de identidades, el correo basura, los programas maliciosos, la explotación y el abuso de niños y otros riesgos pueden tener consecuencias dramáticas, a veces devastadoras, en el mundo real, más allá de los 400.000 millones de dólares de pérdidas estimadas de la economía global (UIT, 2014).

El diseño de aplicaciones capaces de camuflarse en juegos inofensivos que posteriormente, descargan un componente malicioso. La salida al mercado de grandes cantidades de nuevas aplicaciones propicia que cada vez sean más los cibercriminales que prueban suerte en conseguir esquivar el férreo control impuesto por la App Store (Diario ABC Tecnología, 2016).

El Banco Interamericano de Desarrollo (BID) y la Organización de los Estados Americanos (OEA) indicó en un estudio realizado en América Latina, que "cuatro de cada cinco países de la región no tienen estrategias de ciberseguridad o planes de protección de infraestructura crítica, dos de cada tres no cuentan con un centro de comando y control de seguridad cibernética y la gran mayoría de las fiscalías carece de capacidad para perseguir los delitos cibernéticos, entre otras carencias" (El Financiero, 2017)

A nivel regional, varios países han implementado políticas y estrategias sobre ciberseguridad en base a sus líneas base. En la Tabla 1, se puede visualizar los países de América Latina y el caribe que han publicado sus respectivas estrategias y políticas referentes a Ciberseguridad:

Tabla 1

Políticas y estrategias de Ciberseguridad en los países de América Latina y el Caribe

País	Nombre	Año de publicación
Colombia	Política Nacional de Seguridad Digital	2016
Panamá	Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas	2013
Paraguay	Plan Nacional de Ciberseguridad	2016
Costa Rica	Estrategia Nacional de Ciberseguridad	2017
Chile	Política Nacional de Ciberseguridad	2017
México	Estrategia Nacional de Ciberseguridad	2017
República Dominicana	Estrategia Nacional de Ciberseguridad	2018
Guatemala	Estrategia Nacional de Ciberseguridad	2018

Fuente: (Hernández, 2018)

Ecuador no es ajeno al caso de los ciberataques, y por tal razón se ha empezado a trabajar en proteger al país. En 2002 cuando se aprobó la Ley de Comercio Electrónico publicada mediante Registro Oficial 557 del 17 de abril, se realizaron reformas al Código Penal, en las que se incluyeron tipificaciones de delitos informáticos como: acceso no autorizado, falsificación informática, fraude informático, daño informáticos y violación al derecho a la intimidad.

El Código Orgánico Integral Penal del Ecuador (COIP) publicado en el 2014 ha incluido delitos que involucran al acoso mediante medios electrónicos a niños, niñas y adolescentes y pornografía infantil, por lo que se evidencia un avance en el tema penal, pero es necesario establecer el impacto de estas normas en la actividad delincuencial en el Ecuador. (Acurio Del Pino, Panorama legal sobre ciberseguridad en el Ecuador, 2017)

El Índice Global de Ciberseguridad (GCI) emitido por la UIT (Unión Internacional de Telecomunicaciones) y publicado el 6 de julio de 2017, señala que 96 países están en etapa de iniciación en cuanto a los avances de seguridad en la red. El estudio cita que 77 naciones están en la fase de maduración y 21 países lideran la categoría. El Ecuador se encuentra ubicado en el puesto 66 del ranking global, es sexto entre los países de América Latina y el Caribe y ha sido considerado con un nivel maduro. (UIT, 2017)

En el Ecuador se cuenta con el Centro de Respuesta a incidentes informáticos del Ecuador (EcuCERT), creado mediante Resolución ST-2014-0247 del 18 de julio de 2014 por la Ex - Superintendencia de Telecomunicaciones. Es reconocido como un CIRT (Critical Incident Response Team) nacional oficial de acuerdo al Índice mundial de ciberseguridad y perfiles de ciberbienestar. (UIT, 2015)

El EcuCERT, que pertenece a la ARCOTEL (Agencia de Regulación y Control de las Telecomunicaciones) es un CSIRT que permite apoyar a la prevención y resolución de incidentes de seguridad informática mediante la coordinación, capacitación y el soporte técnico. Es necesario sin embargo, determinar el impacto de su accionar en las situación actual que vive el país, especialmente por las limitaciones en sus competencias, que la Ley Orgánica de Telecomunicaciones establece. (ARCOTEL, 2018)

1.2 Planteamiento del problema

1.2.1 Introducción

El problema principal que aborda la Política Nacional de Ciberseguridad es la incertidumbre de su estado actual, presentada desde un método sistemático, con visión crítica e independiente que brinde información pertinente, relevante y veraz de aspectos como:

- La definición de infraestructuras críticas del Estado.
- La investigación académica en temas de seguridad de la información, la implementación de laboratorios y la investigación a nivel de Universidades, número y disponibilidad de expertos en seguridad de la información que contribuyan en el fortalecimiento de este tema.
- Campañas de capacitación sobre seguridad de la información a usuarios finales para la ciudadanía.
- Código Orgánico Integral Penal vigente, respecto de la tipificación de ciertos delitos y el fortalecimiento de penas referentes a ellos.
- Gestión del EcuCERT, considerando las competencias de regulación y control de ARCOTEL otorgadas por la Ley Orgánica de Telecomunicaciones.

- Comité Nacional de Seguridad de la Información y estrategias para fortalecer a la Ciberseguridad nacional.
- Entidades operativas relacionadas con la Seguridad de la Información.
- Cooperación y unificación de competencias de las instituciones responsables en la Ciberseguridad y ciberdefensa.
- Cooperación internacional de lucha contra el cibercrimen y protección de infraestructuras críticas.

1.2.2 Justificación, importancia y alcance

La línea base de Ciberseguridad en el Ecuador permitirá contar con un panorama claro, donde se podrá establecer una visión de futuro de la Ciberseguridad Nacional y determinar la brecha que separa la realidad actual y le proyección de futuro.

Es de vital importancia para que más adelante se pueda diseñar una Política Nacional de Ciberseguridad o Estrategia Nacional que dicte las acciones necesarias para la protección adecuada a las infraestructuras críticas nacionales, sin dejar de lado de ninguna manera la protección que requiere el ciudadano en particular como usuario de la tecnología y de los servicios de E-Government que le proporcione el estado para cumplir con los mandatos constitucionales referente a las garantías de los derechos respecto a estas actividades que ha sido establecidas en la Carta Magna.

La elaboración de este documento formal requiere un sustento metodológico de carácter sistemático que se inicia con un proceso muy importante que es el establecimiento de la línea base del situación actual de alcance nacional, sin el que es imposible partir al diseño de una situación futura, por tanto, este proyecto es de trascendental importancia en la planificación nacional y más que todo en la seguridad del Estado y como parte de este todos los ciudadanos.

1.2.3 Objetivo general del proyecto.

Definir la línea base de la Ciberseguridad en el Ecuador para coadyuvar en el establecimiento de una Política/Estrategia Nacional que incorpore lineamientos, acciones estratégicas, niveles de seguridad en el ciberespacio y protección de los usuarios de los servicios que brinda la tecnología de la información y comunicación.

1.2.4 Objetivos específicos del proyecto

- Establecer un contexto sistemático y actual de la Cibeseguridad en el Ecuador a través de una investigación documental y bibliográfica.
- Identificar los factores que definirán los objetivos del Plan de Investigación de Campo y los instrumentos relacionados.
- Identificar las acciones realizadas por las entidades competentes en el Ecuador referentes a Ciberseguridad.
- Comprender el estado actual de la Ciberseguridad que servirá como base para establecer lineamientos de política o acciones estratégicas para fortalecer el Ciberespacio.
- Establecer el diagnóstico de la Ciberseguridad de una forma sistemática y comprensible en un informe para la difusión del trabajo realizado.

CAPÍTULO II. MARCO TEÓRICO

2.1 Seguridad de la Información

Es necesario establecer que la información es un activo muy importante para cualquier organización y debe ser protegido. Este activo se encuentra expuesto a las amenazas del entorno e internas y generalmente mantiene vulnerabilidades que comprometen a su confidencialidad, integridad y disponibilidad, siendo los tres aspectos importantes que definen la seguridad de la información.

"La seguridad de la información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales." (ISO, 2005)

Además, la seguridad de la información debe contar con tres cualidades fundamentales:

- Crítica
- Valiosa
- Sensible

2.2 Seguridad Informática

Se puede definir como la disciplina que se encarga de diseñar los estándares, procedimientos, métodos y técnicas, orientados a garantizar condiciones para el tratamiento de los datos, la información en los sistemas informático de manera segura y confiable. (Rodríguez A. , 2016)

Por lo tanto, la seguridad informática comprende el uso de antivirus, firewalls, IPS, IDS, etc. También como otras medidas que los usuarios deben tomar como la activación y

desactivación de ciertas funciones de software como scripts de Java y un correcto buen uso de las Tecnologías de la Información, las redes y el Internet.

Según (Universidad Internacional de Valencia, 2016), las medidas que se pueden tomar para garantizar la seguridad informática son:

- La instalación de software legalmente adquirido, ya que este software se encuentra libre de troyanos o virus.
- Los Suites antivirus, con las reglas de configuración y de los sistemas adecuadamente definidos.
- Incorporación de hardware y software firewalls, ya que ayudan con el bloqueo de usuarios no autorizados que intentan acceder a los equipos terminales o a la red.
- Correcto uso de políticas de contraseñas, siendo estas complejas y grandes, y deben constar de varios caracteres especiales, números y letras.
- Cuidado con la ingeniería social a través de las redes sociales, ya que los ciberdelincuentes pueden intentar obtener datos e información que pueden utilizar para realizar ataques.
- Criptografía, especialmente la encriptación: para mantener nuestra información sensible, segura y secreta.

(Universidad Internacional de Valencia, 2016)

2.3 Ciberespacio

El ciberespacio se entiende como el medio donde se interconectan diferentes dispositivos por redes de información, en donde se procesa, manipula, y explota la información, facilitación y el aumento de la comunicación e interacción de individuos.

Según (Machín Osés & Gazapo Lapayese, 2016), el ciberespacio se componen de cuatro elementos fundamentales, tal y como muestra la Figura 1.

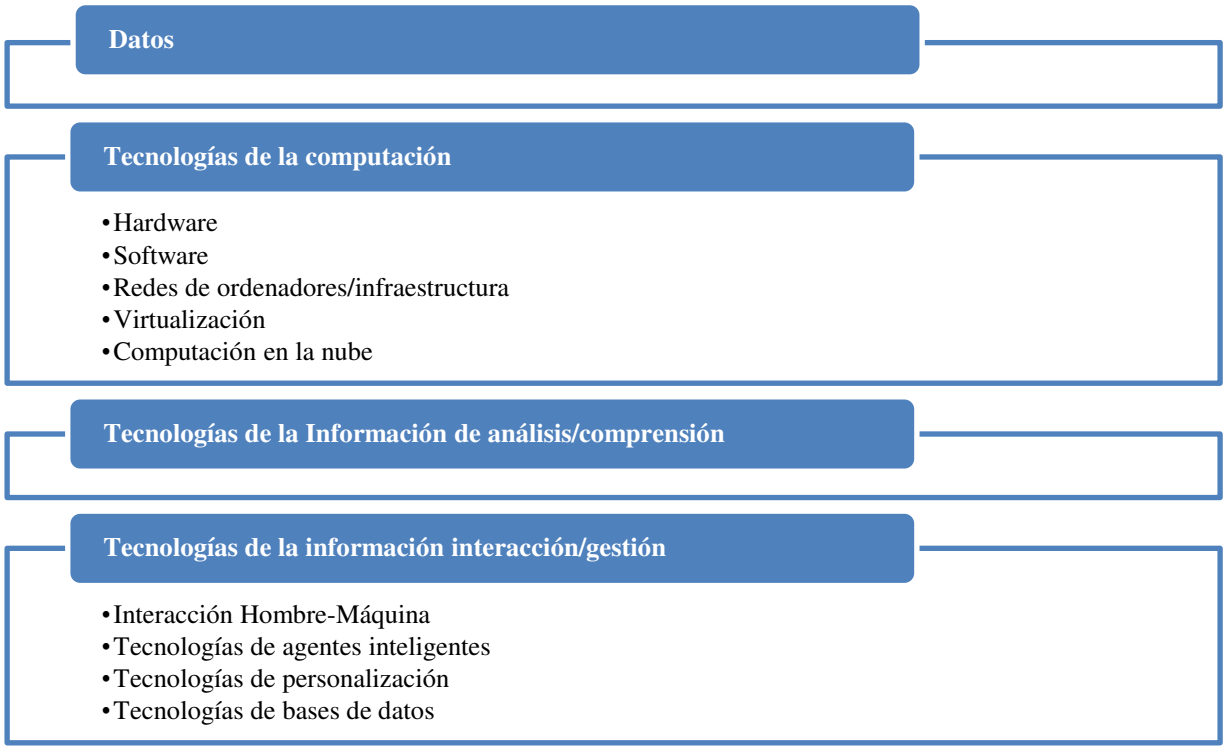


Figura 1. Elementos del ciberespacio
Fuente: (Machín Osés & Gazapo Lapayese, 2016)

Esto nos da a entender, que el ciberespacio es la interconexión de las personas a través de las telecomunicaciones, independientemente del lugar que se encuentren.

Por tal motivo, la información que se encuentra en el ciberespacio es vulnerable a ciberataques, donde el ciberdelincuente ataca contra uno o más de los cuatro elementos mostrados anteriormente.

2.4 Ciberdefensa

De acuerdo a (CARI, 2013), la ciberdefensa “es el conjunto de acciones y/u operaciones activas o pasivas desarrolladas en el ámbito de las redes, sistemas, equipos enlaces y personal de los recursos informáticos y teleinformaticos de la defensa a fin de asegurar el cumplimiento de las misiones o servicios para los que fueran concebidos a la vez que se impide que fuerzas enemigas los utilicen para cumplir los suyos”.

En el Ecuador, el Comando de Ciberdefensa (COCIBER) del Comando Conjunto de las Fuerzas Armadas del Ecuador (COMACO) es el encargado de desarrollar estrategias y acciones de ciberdefensa que permitan defender la infraestructura crítica, las redes y la información electrónica en el ámbito de ciberdefensa. (MICS, 2014)

2.5 Ciberseguridad

Según ISACA (como se citó en Mendoza, 2015), la ciberseguridad se puede definir como la protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados. (ISACA, 2014)

A diferencia de la Seguridad de la Información, la ciberseguridad se enfoca exclusivamente en la protección de la información digital que se encuentra en los sistemas interconectados. (Mendoza, 2015)

De acuerdo a la (ISO, 2010), el enfoque de la ciberseguridad y la manera de confrontar sus riesgos involucra una combinación de múltiples estrategias considerando varias partes involucradas. Estas estrategias incluyen:

- Las mejores prácticas de la industria, con la colaboración de todas las partes interesadas para identificar y abordar los problemas y riesgos de ciberseguridad;
- Una amplia educación hacia consumidores y empleados, proporcionando un recurso confiable sobre cómo identificar y abordar riesgos específicos de Ciberseguridad dentro de la organización y en el ciberespacio; y
- Soluciones tecnológicas innovadoras para ayudar a proteger a los consumidores de los conocidos ataques de ciberseguridad, mantenerse actualizados y estar preparados contra nuevas explotaciones.

Además, el enfoque se da hacia los proveedores de servicios en el ciberespacio, así como por las organizaciones que proporcionan educación relacionada con esta hacia los consumidores, para preparar materiales para una amplia educación hacia el usuario. El detalle de este enfoque se muestra en la Figura 2.

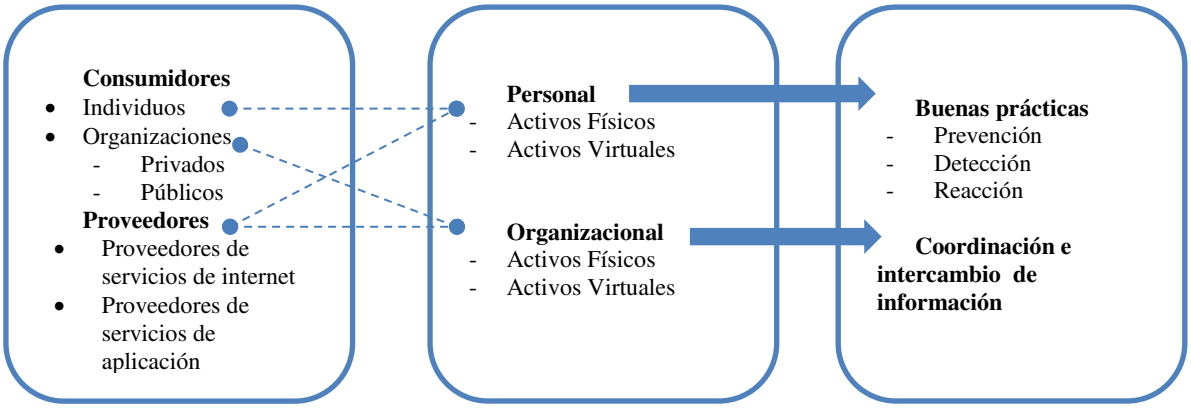


Figura 2. Enfoque de la Ciberseguridad
Fuente: (ISO, 2010)

2.6 Principios de Ciberseguridad

Dentro de los conceptos de Seguridad Informática y Ciberseguridad, que forman parte de la Seguridad de la Información, se definen los principios que todo sistema informático debe contar:

- Confiabilidad. Este concepto hace referencia a la privacidad de la información almacenados y procesados en un sistema informático.
- Integridad. Se hace referencia a la validez y consistencia de los elementos de información almacenados y procesados en un sistema de información.
- Disponibilidad. Hace referencia a la validez y consistencia de los elementos de información almacenados y procesados en un sistema informático.

(Londoño Forero, 2014)

2.7 Infraestructura crítica

Según la Agencia Nacional de Seguridad (NSA) de los Estados Unidos, “es aquella cuyos activos, sistemas y redes, ya sean físicos o virtuales, son tan vitales para el país que su incapacidad o destrucción tendrían un efecto debilitante sobre la seguridad física, económica o pública, la salud, o cualquier combinación de estas. (ESET, 2017)

Estas comprenden más de 3000 instalaciones e infraestructuras sensibles dentro de las siguientes áreas estratégicas:

- Energía: Centrales de producción y redes de distribución de energía.
- Industria Nuclear: Centrales de producción y almacenamiento de residuos.
- Tecnológicas de la Información TIC.
- Infraestructuras del Transporte: Aeropuertos, puertos, ferrocarriles, redes de transporte público, sistemas de control del tráfico, etc.
- Suministro de Agua: Embalses, almacenamiento, tratamiento y redes de distribución.
- Salud: Centros sanitarios, hospitales, laboratorios, etc.
- Sistema Financiero y Tributario: Infraestructura financiera y económica.
- Industria Química: Producción, almacenamiento y transporte de mercancías peligrosas (materiales químicos, biológicos, radiológicos y nucleares).
- Alimentación: Producción, transporte, almacenamiento y distribución.
- Administración: Servicios públicos básicos, instalaciones, redes de información, activos, y principales lugares y monumentos nacionales y patrimonio.

(COCIBER, 2018)

2.8 Ciberataques

Un ciberataque se considera cualquier tipo de maniobra ofensiva hecha por individuos u organizaciones, cuyo objetivo son los sistemas de información como infraestructuras, redes de información, o bases de datos que están alojadas en servidores remotos. Los ciberataques son realizados por medio de actos maliciosos usualmente originados de fuentes anónimas y direcciones que no pueden ser rastreadas.

Según (RCG Comunicaciones, 2018), existen diferentes tipos de ataques informáticos, el cual son necesarios de identificarlos, además de ser los más comunes en los últimos años.

El Malware es un término genérico para referirse a un software malicioso el cual se infiltra a un sistema para dañarlo. Los malwares tienen diferentes variedades donde se pueden identificar virus, gusanos, troyanos, etc. (RCG Comunicaciones, 2018)

Los tipos de Malware que se pueden definir son los siguientes:

- Los virus son códigos maliciosos que infectan los ficheros del sistema, siendo ejecutados por los mismos usuarios. Cuando se ejecuta el virus, este se extiende a otros archivos del sistema i otros sistemas a través de unidades de almacenamiento.
- Los gusanos son programas que realizan copias de sí mismo y se reproducen por medio de las redes de información. Son difíciles de detectar ya que no afectan el funcionamiento normal del sistema.
- Los troyanos son similares a los virus, pero su objetivo es buscar la apertura para la instalación de otros programas maliciosos.
- El Spyware es un programa espía que busca obtener información, su trabajo es silencioso sin mostrar su funcionamiento.

- El Adware es un malware cuya función es mostrar publicidad, este puede recopilar y transmitir datos.
- El Ransomware es un tipo de ciberataque diseñado para obtener un beneficio monetario de una víctima. Este exige un pago para deshacer los cambios que el virus troyano haya realizado en la computadora de la víctima. Estos cambios pueden ser: Cifrar datos almacenados en el disco de la víctima, para que esta no pueda acceder a la información, o bloquear el acceso normal al sistema de la víctima.

  Estos ataques se instalan a través de correos electrónicos maliciosos (phishing) o como consecuencia de visitar una página web con contenido malicioso. Una vez instalado, el troyano cifra la información almacenada en la computadora de la víctima o bloquea la computadora para que no funcione normalmente, dejando un mensaje de recuperación exigiendo el pago de una tarifa para descifrar los archivos o restablecer el sistema. (Kaspersky Lab, 2018)

En el 2017, el mundo ha sido víctima de ataques cibernéticos más potentes y mejor desarrollados a gran escala de las cuales destacan:

- Filtraciones de Shadow Brokers. En abril de 2017 un grupo de hackers conocido como Shadow Brokers realizaron revelaciones sobre las herramientas de la Agencia Nacional de Seguridad (NSA), en la que incluía una vulnerabilidad de Windows conocido como EternalBlue, que hackers aprovecharían después en dos de los ataques de ransomware más importantes de 2017.
- WannaCry. Un ransomware masivo que atacó a empresas y particulares de todo el mundo, causando problemas en grandes corporaciones y organismos públicos.
- Petya. Un ransomware más avanzado que Wannacry aprovechó las vulnerabilidades de Windows expuestas por Shadow Brokers y alcanzó objetivos de todo el mundo.

A nivel mundial, estos datos reflejan un crecimiento de ciberataques y exposiciones de vulnerabilidades en las instituciones. Por tal motivo se han realizado cooperaciones entre los gobiernos y organismos internacionales para determinar con cifras la situación actual de los países y de las regiones. Esto permitirá tomar acciones regionales y locales como políticas y estrategias nacionales.

En Ecuador de acuerdo al EcuCERT, se han detectado diferentes amenazas de las cuales podemos citar:

- Listas negras. Son listas de direcciones IP que representan un posible peligro por la generación de spam.
- Fuerza bruta. Es una práctica de prueba y error que prueba todas las combinaciones posibles para obtener información personal como contraseñas o números de identificación personal.
- Sitios web comprometidos. Son páginas web infectadas con código malicioso que representan un peligro a sus visitantes, con el fin de obtener información de las víctimas como credenciales de inicio de sesión o cuentas bancarias.
- Botnet. Son conjunto de host conectados a Internet que interactúan para cumplir una tarea específica de manera ilícita, siendo controlados sin el consentimiento de los propietarios de los hosts.
- Spam. También conocido como “correo basura”, son mensajes no solicitados con el fin de realizar publicidad de un producto o servicio.

(ARCOTEL, 2018)

CAPÍTULO III. PROCESO DE LA INVESTIGACIÓN

3.1 Planificación de la investigación

Para determinar la planificación de la investigación y desarrollar la línea base de Ciberseguridad en el Ecuador, es necesario plantear una metodología que nos permita identificar la problemática y las soluciones a las mismas referentes a la Ciberseguridad en el Ecuador.

Para ello, se aplicará la práctica japonesa Tankyu, donde determinaremos dicha planificación.

3.1.1 Práctica Tankyu

La práctica Tankyu es un método que nos permite identificar los problemas referentes a las Tecnologías de la Información y Comunicación. Esta práctica fue desarrollada por el Instituto de Computación de Kobe por el Profesor Toshiki Sumitani.

Los componentes de la Práctica Tankyu son:

- Identificación de problemas sociales
- Desarrollo y aplicación de fortalezas para resolver estos problemas
- Implementación de una solución para esos problemas

(KIC, 2017)

3.1.1.1 Mapa Tankyu

La estrategia de identificación de problemas mediante la Práctica Tankyu se puede visualizar en la Figura 3, donde se muestran los problemas en el Ecuador, las posibles

soluciones que se aplicarían para dichos problemas, el modelo de negocio donde se mencionan las instituciones responsables para su aplicación, los recursos y aplicaciones tecnológicas y recursos humanos. Ver Figura 3

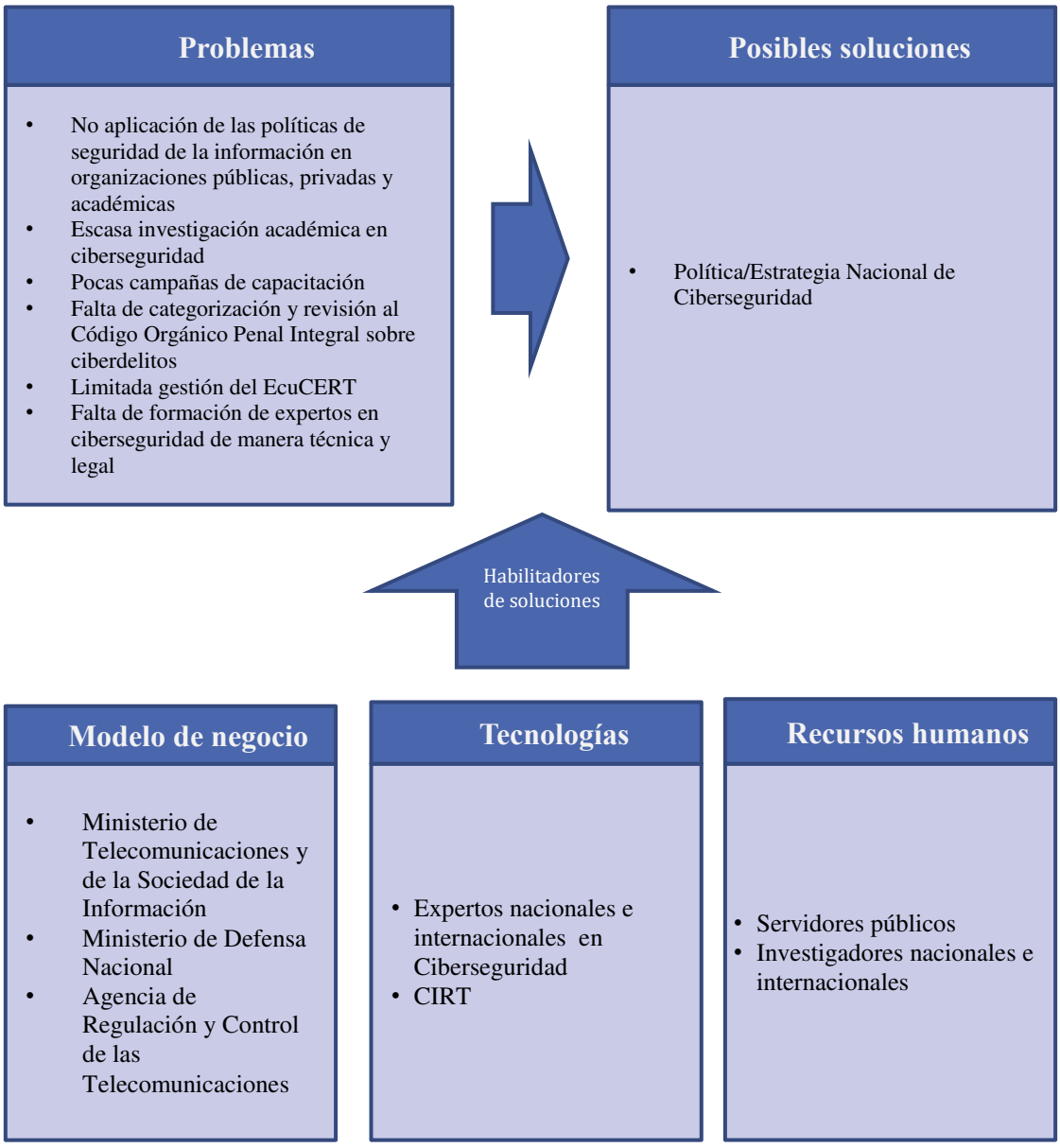


Figura 3. Mapa Tankyu sobre Ciberseguridad en el Ecuador

Como podemos apreciar, existen muchas falencias dentro del campo de la ciberseguridad en el Ecuador, lo que la falta de acciones puntuales nos convierte en un país vulnerable a ataques informáticos. Por tal motivo es necesaria la implementación de una política/ Estrategia Nacional de Ciberseguridad en el Ecuador, pero para poder contar con dicha herramienta normativa, es necesario elaborar la línea base de la Ciberseguridad.

3.1.2 PCM (Project Cycle Management)

El método PCM es una técnica de planificación de proyectos para analizar y resolver un problema existente.

Este método impartido mediante cooperación japonesa (JICA) ha sido desarrollado por The Foundation for Advanced Studies on International Development (FASID).

Desde mediados de la década de 1990, se ha utilizado generalmente en las actividades de cooperación técnica de Japón para planificar y garantizar la ejecución efectiva de los proyectos.

Para desarrollar el Método PCM, es necesario identificar las causas y efectos del problema principal, y con ello construir el árbol de problemas y a partir de este, los objetivos a alcanzar a través de esta problemática. (JICA - KIC, 2017)

La Figura 4 muestra la problemática que el Ecuador tiene referente a la Ciberseguridad, y a partir de allí se formularán los objetivos.

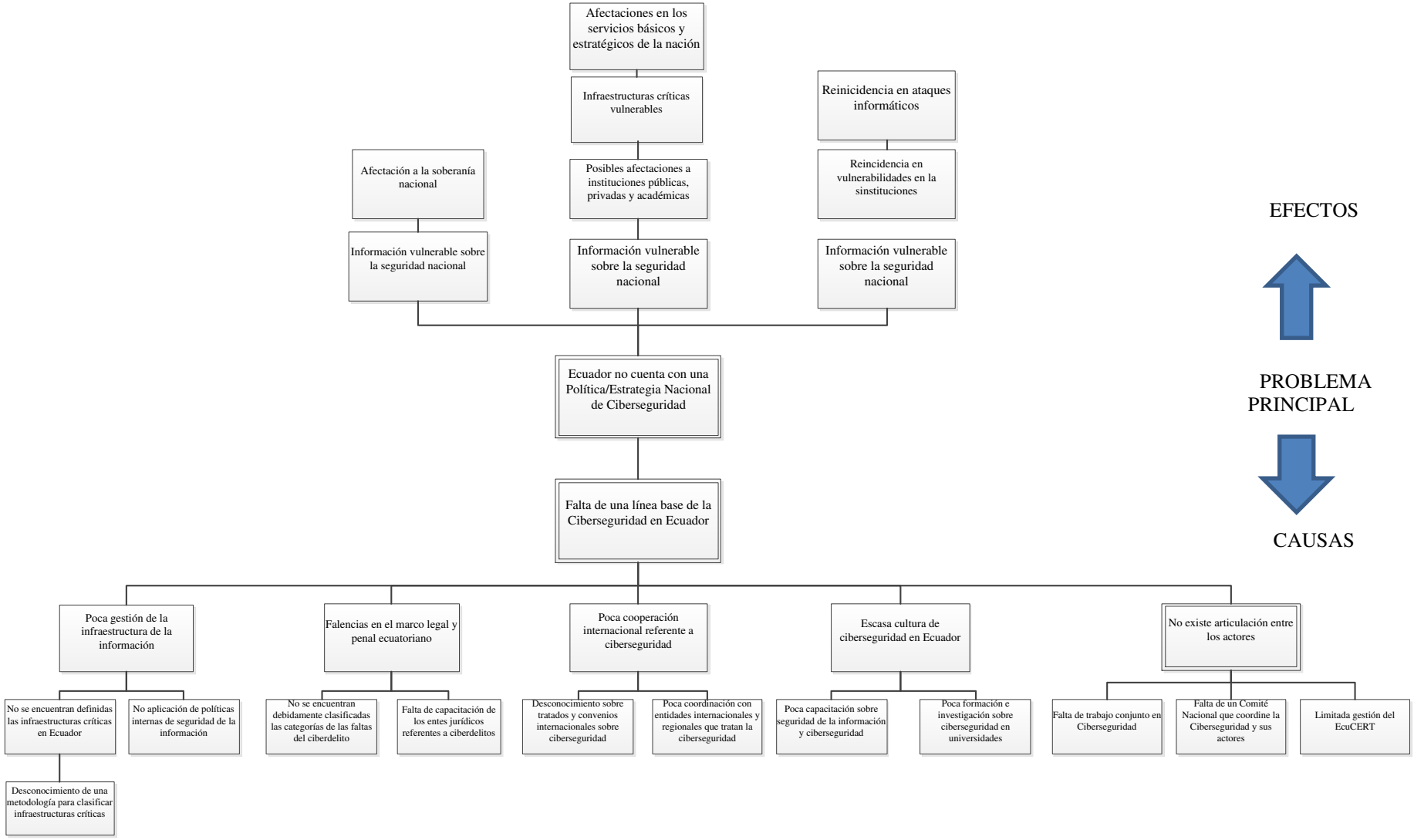


Figura 4. Árbol de problemas sobre ciberseguridad en Ecuador

La problemática principal en el país radica en la ausencia de una Política y/o Estrategia Nacional de Ciberseguridad que permitan dictar las diferentes acciones para poder robustecer los diferentes campos de acción de la ciberseguridad.

Para poder construir dicho documento, es necesario realizar la articulación de las diferentes instituciones competentes del Estado Ecuatoriano, y con un trabajo conjunto entre el sector privado y académico determinar la situación actual de Ecuador.

En base a lo indicado en la Figura 4, se plantean los objetivos principales, en las cuales abordaría la línea base, que servirá para determinar la Estrategia/Política Nacional de Ciberseguridad.

Para ello, se plantea analizar las diferentes áreas:

- Aspectos técnicos
- Aspectos legales
- Aspectos de Cooperación internacional
- Aspectos de formación y capacitación
- Aspectos de institucionalización

Estos aspectos son primordiales para plantear el plan de investigación de campo, donde se identificarán los actores que nos permitirán contar con la información necesaria para elaborar el presente trabajo.

3.1.3 Selección de Factores

En la región, muchos países han establecido sus correspondientes políticas y estrategias nacionales de ciberseguridad. A través de la OEA y la UIT quienes han determinado factores para establecer un modelo de madurez y guías para establecer estrategias de ciberseguridad.

Es necesario agrupar estos elementos que han sido propuestos, con el fin de establecer los factores que se tomarán en cuenta en la investigación de campo, considerando el porcentaje de inclusión de estos factores en los documentos analizados. En la Tabla 2 se puede apreciar los aspectos de interés para la investigación de campo.

Tabla 2

Aspectos de interés para la investigación de campo

ASPECTOS / PAÍS	Cultura y concienciación	Marco legal y regulatorio	Formación y educación	Infraestructuras críticas	Respuesta a incidentes	Institucionalidad y organización	Cooperación y asistencia	Gestión de Riesgo	Investigación e innovación	Coordinación y colaboración	Estándares y criterios técnicos	Gobernanza	Combate al cibercrimen	Desarrollo digital y telecomunicaciones	Industria y tecnología	Infraestructura de la información	Desarrollo de capacidades	Estrategia Nacional	Seguimiento y evaluación	Práctica de los operadores	Promoción de derechos	Impacto económico	Planificación y marco de trabajo	Continuidad operativa
Chile	-							-													-			
Colombia	-							-														-		
Costa Rica	-	-	-	-	-	-	-	-	-	-				-			-		-	-	-	-	-	
Guatemala	-	-	-	-	-	-		-			-	-			-	-		-						
Jamaica	-	-	-	-	-		-	-	-			-							-					
México	-	-		-				-	-	-	-						-		-					
Panamá	-	-	-	-	-				-						-									-
Paraguay	-		-	-	-	-			-	-			-	-		-		-						
República Dominicana	-	-	-	-		-	-																	
Trinidad - Tobago	-	-			-		-					-												
Niveles de madurez OEA	-	-	-	-	-	-		-			-	-	-	-	-	-		-		-	-			
ITU NCSG	-	-	-		-	-	-			-	-													
% Inclusión	100	92	83	83	75	67	58	58	50	42	42	42	33	33	33	33	25	25	25	25	25	17	17	8

Fuente: (Ron, Rivera, Fuertes, Toulkeridis, & Diaz, 2018)

3.1.4 Plan de investigación de campo

Para organizar la información necesaria para consolidar la Línea Base de la Ciberseguridad en el Ecuador, es necesario plantear el Plan de investigación de campo, que se establece a través de los objetivos planteados a través del árbol de problemas descrito en la Figura 4 y en los factores identificados por otros países, se plantea realizar la investigación de campo a través de los siguientes aspectos:

- Estado de la Infraestructura de la Información
- Estado del marco penal
- Estado de la sensibilización, capacitación y formación
- Estado de la cooperación nacional e internacional
- Estado de la Institucionalidad

Los objetivos planteados para la investigación de campo permitirán responder las inquietudes referentes a la situación actual de la Ciberseguridad son:

a) Determinar la gestión y ámbito de empleo del Comando de Ciberdefensa (COCIBER) de las Fuerzas Armadas, como parte de la información necesaria para determinar la Línea Base de la Ciberseguridad en el Ecuador.
b) Conocer el estado de las políticas internas en el sector público, privado, académico en el Ecuador
c) Conocer el número de incidentes y vulnerabilidades reportados por el EcuCERT
d) Conocer las estadísticas de los ciberdelitos en Ecuador y las capacidades de los fiscales en relación del ciberdelito.
e) Conocer las asociaciones internacionales que se cuenta en el Ecuador para prevenir y contrarrestar ataques informáticos
f) Identificar los aspectos relacionados a la formación de profesionales en ciberseguridad
g) Organizar la Institucionalización de la Ciberseguridad

Las preguntas que nos permitirán recopilar la información necesaria se muestra en la Tabla 3, donde se detalla los objetivos, los temas de interés, las preguntas básicas que se necesita conocer y la entidad que proporcionará dicha información.

Tabla 3

Planteamiento de variables del Plan de investigación de campo

No.	OBJETIVOS	TEMAS DE INTERÉS	PREGUNTAS BÁSICAS	ENTIDAD RESPONSABLE
1	Determinar la gestión y ámbito de empleo del Comando de Ciberdefensa (COCIBER) de las Fuerzas Armadas, como parte de la información necesaria para determinar la Línea Base de la Ciberseguridad en el Ecuador.	Modelo de gestión, metodologías y clasificación	¿Cuál es el modelo de Gestión de su Organización, su misión, alcance, cobertura, funciones técnicas principales, capacidades, infraestructura, personal con el que cuenta, su formación, capacitación y necesidades actuales urgentes?	Comando de Ciberdefensa
			¿Cuál es la metodología utilizada para la clasificación y selección de las infraestructuras críticas, la base legal que sustenta esta responsabilidad y las dificultades de implementación e inconsistencias del modelo?	Comando de Ciberdefensa
			¿Cuál es la clasificación actual e identificación de las infraestructuras críticas en el Ecuador?	Comando de Ciberdefensa
		Plan de protección de infraestructuras críticas	¿En qué consiste el Plan de Protección de Infraestructuras críticas, cuáles son las entidades responsables en aplicarlo y cuáles los inconvenientes en su aplicación?	Comando de Ciberdefensa
		Aportes	¿Cuál sería el aporte y cómo participaría el COCIBER en el establecimiento de la Política Nacional de Ciberseguridad del Ecuador?	Comando de Ciberdefensa
2	Conocer el estado de las políticas internas en el sector público, privado, académico en el Ecuador	Políticas internas en el sector público	¿Cuál es el estado actual del EGSI?	Ministerio de Telecomunicaciones y de la Sociedad de la Información
			¿Cuántas y qué instituciones cuentan con políticas internas sobre seguridad de la información y/o Ciberseguridad?	Ministerio de Telecomunicaciones y de la Sociedad de la Información
			¿Cuántas y qué instituciones cuentan con planes de contingencia ante un incidente informático en las instituciones públicas?	Ministerio de Telecomunicaciones y de la Sociedad de la Información
			¿Cuántas y qué instituciones cuentan con planes de resiliencia ante un incidente informático en las instituciones públicas?	Ministerio de Telecomunicaciones y de la Sociedad de la Información

CONTINÚA

No.	OBJETIVOS	TEMAS DE INTERÉS	PREGUNTAS BÁSICAS	ENTIDAD RESPONSABLE
			¿Cuántas y qué instituciones cuentan con planes de continuidad ante un incidente informático en las instituciones públicas?	Ministerio de Telecomunicaciones y de la Sociedad de la Información
			¿Cuántos oficiales de seguridad (CISO) que existen en el sector público?	Ministerio de Telecomunicaciones y de la Sociedad de la Información
		Políticas internas en el sector privado	¿A qué unidades a quien reporta el CISO?	Deloitte
			¿Cuáles son las áreas bajo la responsabilidad de un CISO?	Deloitte
			¿Existe monitoreo de Seguridad de la Información?	Deloitte
			¿Cuentan con procesos y/o tecnologías de riesgo en Seguridad de la Información?	Deloitte
			¿Su institución dispone de un SOC?	Deloitte
			Observaciones de auditoría	Deloitte
		Políticas internas en el sector Academia	¿Existen políticas de Seguridad de TIC en su universidad?	CEDIA
			¿El responsable de la seguridad de la información es parte del área de TIC?	CEDIA
			¿Se realizan auditorías de seguridad?	CEDIA
			¿Cuentan con un plan de contingencia?	CEDIA
			¿Cuentan con un plan de continuidad?	CEDIA
			¿Cuentan con herramientas de análisis de vulnerabilidades?	CEDIA
3	Conocer el número de incidentes y vulnerabilidades reportados por el EcuCERT	Incidentes de ciberseguridad en el Ecuador	¿Cuántas amenazas han sido detectadas en Ecuador?	Agencia de Regulación y Control de las Telecomunicaciones
			¿Cuántas vulnerabilidades han sido detectadas en el Ecuador?	Agencia de Regulación y Control de las Telecomunicaciones
			¿Qué tipos de ataques informáticos han sido detectados?	Agencia de Regulación y Control de las Telecomunicaciones
4	Conocer las estadísticas de los ciberdelitos en Ecuador y las capacidades de los fiscales en relación del ciberdelito.	Tendencia de los delitos informáticos en el Ecuador	¿Cuántos delitos informáticos han sido denunciados en la Fiscalía General del Estado en los últimos años?	Fiscalía General del Estado
		Capacitación a personal de la Fiscalía General del Estado	¿En qué provincias y en qué año se han impartido capacitaciones sobre ciberdelitos a los fiscales?	Fiscalía General del Estado
			¿Cuáles son las temáticas tratadas en esas capacitaciones?	Fiscalía General del Estado
			¿Cuántos funcionarios fueron capacitados?	Fiscalía General del Estado

CONTINÚA

No.	OBJETIVOS	TEMAS DE INTERÉS	PREGUNTAS BÁSICAS	ENTIDAD RESPONSABLE
5	Conocer las asociaciones internacionales que se cuenta en el Ecuador para prevenir y contrarrestar ataques informáticos	Convenios internacionales	¿Estamos suscritos al Convenio de Budapest?	Ministerio de Telecomunicaciones y de la Sociedad de la Información
			¿Cuáles son las afiliaciones con organizaciones internacionales referentes a Ciberseguridad del EcuCERT?	Agencia de Regulación y Control de las Telecomunicaciones
			¿Cuántos convenios internacionales vigentes tiene el Ecuador para tratar temas de ciberseguridad?	Agencia de Regulación y Control de las Telecomunicaciones
6	Identificar los aspectos relacionados a la formación de profesionales en ciberseguridad.	Sensibilización de la ciberseguridad	¿Qué acciones ha tomado el MINTEL para fomentar la cultura de la ciberseguridad en la ciudadanía?	Ministerio de Telecomunicaciones y de la Sociedad de la Información
		Capacitación de la ciberseguridad	¿Qué tipo de capaciones ha promovido MINTEL sobre la prevención del Internet, ciberseguridad y redes sociales a través de los Infocentros?	Ministerio de Telecomunicaciones y de la Sociedad de la Información
			¿Cuántas capacitaciones sobre seguridad de la información y/o ciberseguridad realizadas por el EcuCERT por años (Nro. de Capacitados, temáticas, etc.)?	Agencia de Regulación y Control de las Telecomunicaciones
		Formación de la Ciberseguridad	¿Cuántas universidades Ecuador cuentan con diplomados/especializaciones/ posgrados/doctorados referentes a Seguridad de la Información y/o Ciberseguridad?	Secretaría de Educación Superior, Ciencia y Tecnología
			¿Cuáles con los diplomados/especializaciones/ posgrados/doctorados sobre seguridad de la información/ciberseguridad en el Ecuador?	Secretaría de Educación Superior, Ciencia y Tecnología
			¿Cuántos estudiantes se encuentran inscritos en estos diplomados/especializaciones/ posgrados/doctorados sobre seguridad de la información/ciberseguridad en el Ecuador?	Secretaría de Educación Superior, Ciencia y Tecnología
			¿Cuántos becarios especialistas en Seguridad de la Información/Ciberseguridad se han formado fuera del país?	Instituto de Fomento al Talento Humano
			¿Cuántos becarios especialistas en Seguridad de	Instituto de Fomento al Talento Humano

CONTINÚA

No.	OBJETIVOS	TEMAS DE INTERÉS	PREGUNTAS BÁSICAS	ENTIDAD RESPONSABLE
			la Información/Ciberseguridad se han trabajan en el país?	
			¿Qué país tiene más demanda en la formación de los becarios especialistas en Seguridad de la Información/Ciberseguridad?	Instituto de Fomento al Talento Humano
			¿Cuáles son las acciones que el Ministerio de Educación ha tomado para incluir la ciberseguridad en la educación de niños y adolescentes?	Ministerio de Educación
7	Organizar la Institucionalización de la Ciberseguridad	Articulación de los actores	¿Cuáles son las entidades responsables de la ciberseguridad?	Ministerio de Telecomunicaciones y de la Sociedad de la Información
			¿Cuáles son las funciones del EcuCERT?	Agencia de Regulación y Control de las Telecomunicaciones

CAPÍTULO IV. LÍNEA BASE DE LA CIBERSEGURIDAD DEL ECUADOR

4.1 Estado de la Infraestructura de la información

4.1.1 Infraestructuras críticas

El Acuerdo Ministerial 281 emitido por el Ministerio de Defensa Nacional el 12 de septiembre del 2014 dispone la creación del Comando de Ciberdefensa como una unidad que forma parte de las Fuerzas Armadas del Ecuador, cuya misión es "proteger y defender la infraestructura crítica e información estratégica del Estado" a través de la planificación y ejecución de las operaciones de ciberdefensa. Estas acciones se deberán llevar a cabo a través de acciones de protección del ciberespacio, prevención, disuasión, explotación y respuesta ante eventuales amenazas, riesgos e incidentes informáticos dirigidos hacia las infraestructuras críticas e información estratégica del Estado.

Esta unidad ha determinado las diferentes infraestructuras críticas en el país de acuerdo a lo definido por el catálogo Nacional de Infraestructuras críticas, pero por la naturaleza de la información, ya que se considera confidencial, no es posible enumerar dichas infraestructuras, ya que podría comprometer a la seguridad nacional.

Según (Guerrero, 2018), existen organizaciones industriales en el Ecuador referentes a los sectores que pueden involucrar infraestructuras críticas, en la Figura 5 se muestra el nivel de sensibilidad de las organizaciones industriales del Ecuador en porcentajes.

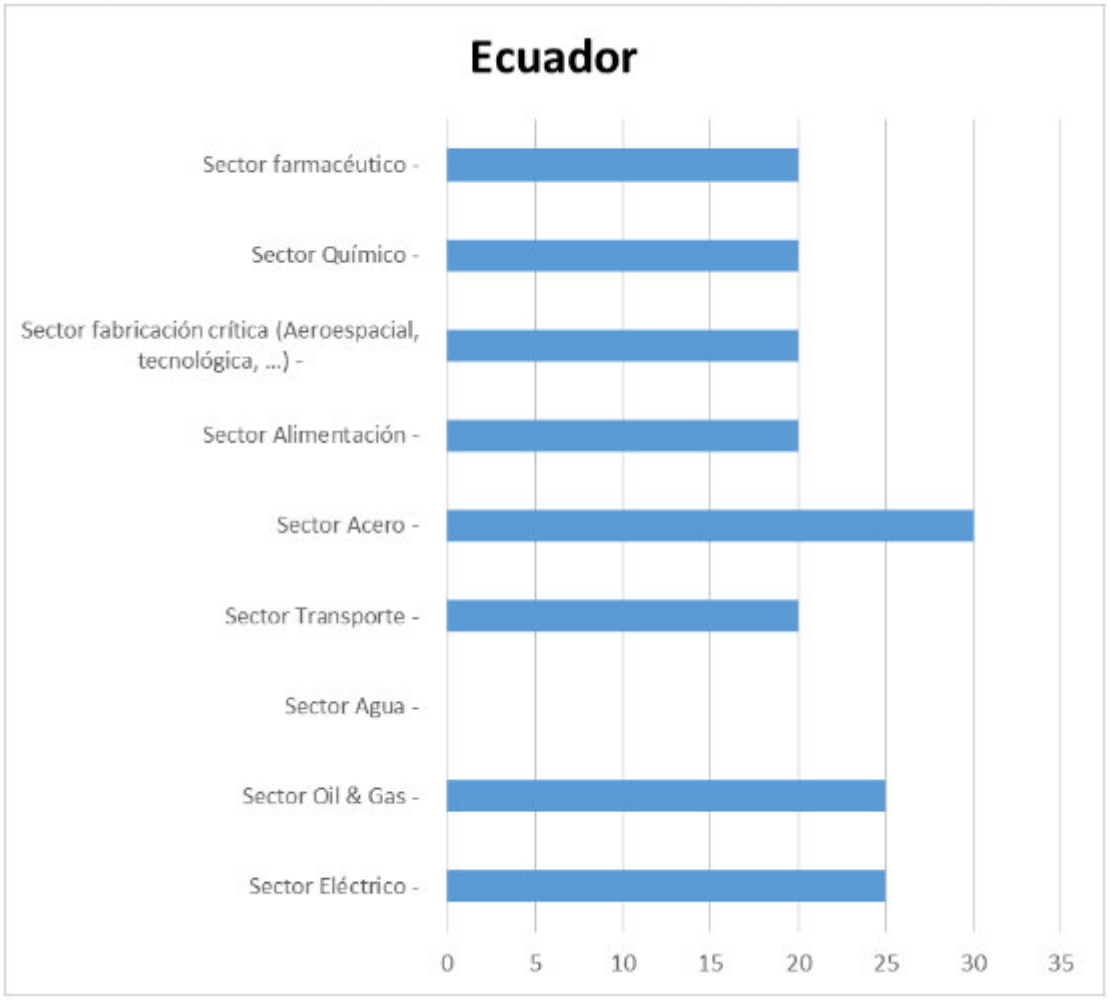


Figura 5. Nivel de sensibilidad de las organizaciones industriales en Ecuador
Fuente: (Guerrero, 2018)

De acuerdo al (COCIBER, 2018), la clasificación de la infraestructuras críticas en el Ecuador se detalla en la Tabla 4.

Tabla 4
Infraestructura crítica estratégica nacional

No.	Infraestructura
1	Telecomunicaciones: Antenas, repetidoras, radares
2	Hidrocarburos: Refinerías, oleoductos, poliductos, bloques petroleros, estaciones, terminales y depósitos, mono boyas, plataformas, almacenamiento GLP, gasoductos.
3	Sector eléctrico: Hidroeléctricas, termo generadoras, eólicas, biomasa
4	Puertos y aeropuertos: Puertos marítimos, aeropuertos

CONTINÚA

No.	Infraestructura
5	Pistas y capitanías: Pistas de despliegue, helipuertos, direcciones regionales de espacios acuáticos, capitanías de puerto, retenes navales

Fuente: (COCIBER, 2018)

Y en base a la sensibilidad de dichas infraestructuras críticas, se clasifican de acuerdo a la siguiente escala de impacto: muy alto, alto, medio y moderado.

Figura 6. Sensibilidad de las infraestructuras críticas en el Ecuador
Fuente: (COCIBER, 2018)

De acuerdo (Aguirre Ponce, 2017) a En Ecuador, muchos sectores vitales han puesto énfasis en temas de ciberseguridad, de las cuales se puede mencionar:

- Sector financiero
- Sector Gobierno
- Sector Telecomunicaciones
- Sector Defensa

Menciona además, que la mayoría de los sectores vitales son brindados a través de las instituciones públicas, donde es posible fortalecer dichas infraestructuras con la aplicación del Acuerdo 166 emitido por la SNAP en el 2014, pero los controles que se establecen en la

implementación de la Esquema Gubernamental de la Seguridad de la Información (EGSI) no cubre de forma integral todos los controles de ciberseguridad. (Aguirre Ponce, 2017)

El COCIBER no evidencia información solicitada en el instrumento de investigación LBCE-IIC-01 su modelo de gestión de la organización, personal, formación, capacitación y necesidades, tampoco se evidencia la metodología que dicha entidad utiliza para la definición, clasificación e identificación de infraestructuras críticas en el país, así como sobre el Plan de Protección de Infraestructuras críticas.

4.1.2 Políticas internas en el sector público

La Secretaría Nacional de Administración Pública (SNAP), emitió el Acuerdo Ministerial No. 166 del 19 de septiembre de 2013 donde indica a las entidades de la Administración Pública Central, Institucional y Dependiente de la Función Ejecutiva (APCID) la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI) mediante la aplicación NTE INEN ISO/IEC 27002 “Código de Buenas Prácticas para la Gestión de la Seguridad de la Información”.

Además, el Acuerdo Ministerial dispone que las entidades de la APCID “que generan, utilizan, procesan, comparten y almacenan información en medio electrónico o escrito, clasificada como pública, confidencial, reservada y no reservada, deberán aplicar el Esquema Gubernamental de Seguridad de la Información para definir los procesos, procedimientos y tecnologías a fin de garantizar la confidencialidad, integridad y disponibilidad de esa información, en los medios y el tiempo que su legitimidad lo requiera". (SNAP, 2013)

Como Evidencia O-02 recopilada mediante el instrumento de investigación LBCE-IIC-02 (Ver Anexo C), se muestran la siguiente información.

De acuerdo a la Subsecretaría de Gobierno Electrónico del Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), la evaluación de la aplicación del EGSI se la realizó en 2 fases:

- Fase 1, donde se implementan 126 hitos prioritarios el EGSI donde han sido evaluados 115 instituciones.
- Fase 2, donde se implementan hitos no prioritarios escogidos por las entidades de acuerdo a la función que cada una desempeña, y 113 instituciones han sido evaluadas en esa etapa.

Al final, MINTEL evaluación la aplicación del EGSI a las entidades que aplicaron las Fases 1 y 2. (MINTEL, 2018)

La evaluación de los controles se determinará de acuerdo al nivel de cumplimiento y a la ponderación que conlleva. La Figura 7 muestra los niveles de calificación de acuerdo a su ponderación.

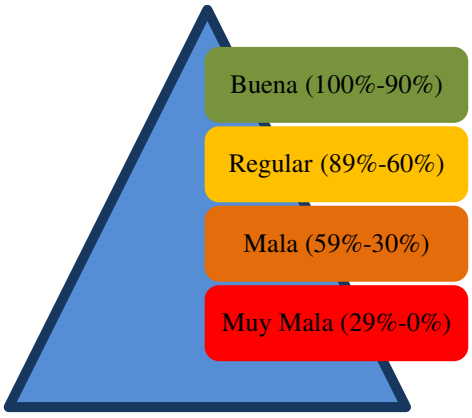


Figura 7. Niveles de calificación del EGSI
Fuente: (MINTEL, 2018)

De acuerdo al (MINTEL, 2018) hasta agosto de este año, se han evaluado a 64 de instituciones de la APCID, de las cuales sólo el 15.63% obtuvo un resultado bueno en el cumplimiento del EGSI, el 71.88% logró un resultado regular, mientras que el 10.94% obtuvo un calificación mala; y el 1.56%, muy mala.

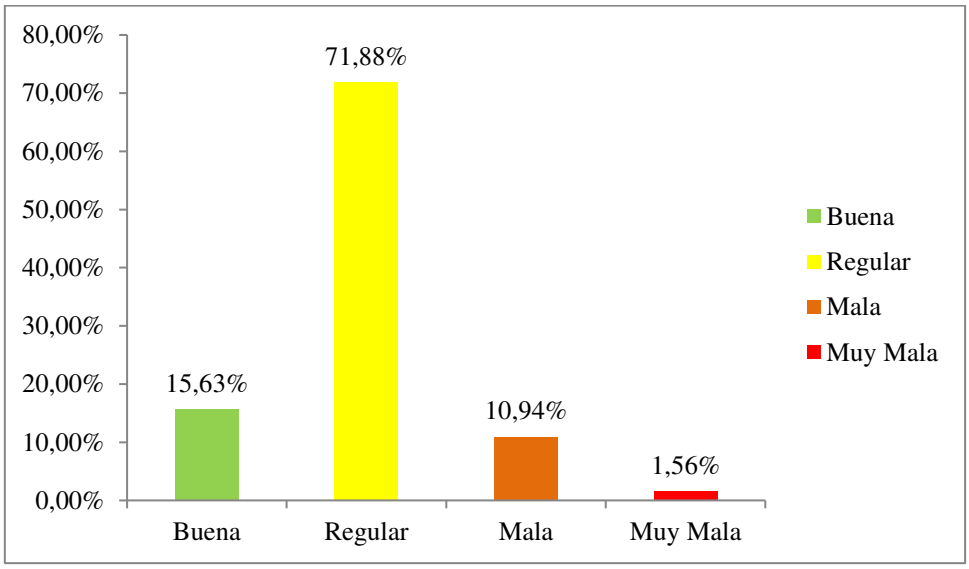


Figura 8. Cumplimiento del EGSI en Ecuador
Fuente: (MINTEL, 2018)

Según (MINTEL, 2018) a agosto del 2018, las 64 instituciones evaluadas en las Fases 1 y 2 cuentan con Políticas de Seguridad internas, donde se valuaron que dichas políticas se encuentren actualizadas, y en el caso de que no lo estén, la Subsecretaría de Gobierno Electrónico realizó las recomendaciones respectivas para la revisión y actualización anual.

Dentro de la Fase 1 del EGSI no se contempla la evaluación del Plan de Contingencia como un hito prioritario, por lo que en la Fase 2 se podría considerar un hito opcional. Al no considerarse como un hito el contar con un Plan de Contingencia ante un incidente prioritario, no se cuenta actualmente con esa información.

Existe un dominio en el EGSI denominado “Gestión de los incidentes de la seguridad de la información” donde existe un control prioritario obligatorio denominado “Reporte sobre los eventos de seguridad de la información” donde es necesario el cumplimiento de los siguientes puntos:

“(*) Instaurar un procedimiento formal para el reporte de los eventos de seguridad de la información junto con un procedimiento de escalada y respuesta ante el incidente, que

establezca la acción que se ha de tomar al recibir el reporte sobre un evento que amenace la seguridad de la información.

(*) Cuando un incidente se produzca, el funcionario en turno responsable del equipo o sistema afectado, debe realizar las siguientes acciones en su orden:

- *Identificar el incidente*
- *Registrar el incidente en una bitácora de incidentes (reporte de eventos) incluyendo fecha, hora, nombres y apellidos del funcionario en turno, departamento o área afectada, equipo o sistema afectado y breve descripción del incidente*
- *Notificar al Oficial de Seguridad de la Información de la institución*
- *Clasificar el incidente de acuerdo al tipo de servicio afectado y al nivel de severidad*
- *Asignar una prioridad de atención al incidente en el caso de que se produjeran varios en forma simultanea*
- *Realizar un diagnóstico inicial, determinando mensajes de error producidos, identificando los eventos ejecutados antes de que el incidente ocurra, recreando el incidente para identificar sus posibles causas*
- *Escalar el incidente en el caso que el funcionario en turno no pueda solucionarlo, el escalamiento deberá ser registrado en la bitácora de escalamiento de incidentes. El funcionario en turno debe escalar el incidente a su jefe inmediato, en el caso en el que el funcionario no tuviere un jefe al cual escalarlo, este debe solicitar soporte al proveedor del equipo o sistema afectado*
- *Investigar y diagnosticar en forma definitiva las causas por las cuales se produjo el incidente*
- *Resolver y restaurar el servicio afectado por el incidente debido a la para de un equipo o un sistema, incluyendo un registro de la solución empleada en la bitácora de incidentes*

- *Cerrar el incidente, actualizando el estado del registro del incidente en la bitácora de incidentes a "Resuelto". Confirmar con el funcionario en turno, responsable del equipo o del sistema de que el incidente ha sido resuelto"* (MINTEL, 2018)

De acuerdo al (MINTEL, 2018), no existe un dominio que contenga evaluaciones sobre planes de resiliencia, pero dentro del hito denominado "Gestión de los incidentes de la seguridad de la información" donde se evalúa la manera de como reportar un incidente informático, su tratamiento y solución. Por tal motivo, no se cuenta con una estadística que identifique un estado actual sobre este aspecto.

Sobre planes de continuidad, existe un dominio que trata sobre la "Gestión de la continuidad del negocio", donde existen varios hitos relacionados a este tema. Estos hitos son no prioritarios y opcionales evaluados en la Fase 2. En las evaluaciones se han observado muy pocas instituciones que han implementado algún hito de este capítulo por lo que no se cuenta con esta información. (MINTEL, 2018)

En cumplimiento del EGSI, existen 125 oficiales de seguridad de las entidades de la APCID donde entidades como empresas públicas e instituciones que no forman parte de la APCID solicitaron ser parte del EGSI. (MINTEL, 2018)

4.1.3 Políticas internas en el sector privado

Como Evidencia O-09 recopilada mediante el instrumento de investigación Informe de la Seguridad de la Información 2017 presentado por la empresa Deloitte, se presente un estudio realizado más de 50 empresas nacionales y multinacionales, que se encuentran las que prestan servicios financieros, bienes de consumo, energía y recursos renovables, tecnología, medios y telecomunicaciones y ciencias de la salud en el Ecuador sobre su gestión sobre la seguridad de la información. (Deloitte, 2017)

El informe indica que el 79% de las entidades encuestadas, cuenta con un responsable de seguridad de la información (CISO[1]) o similar, mientras que el 21% no cuenta.

De ese 79%, el nivel de escalamiento de reporte de un incidente por parte del CISO se muestra en la Figura 9.

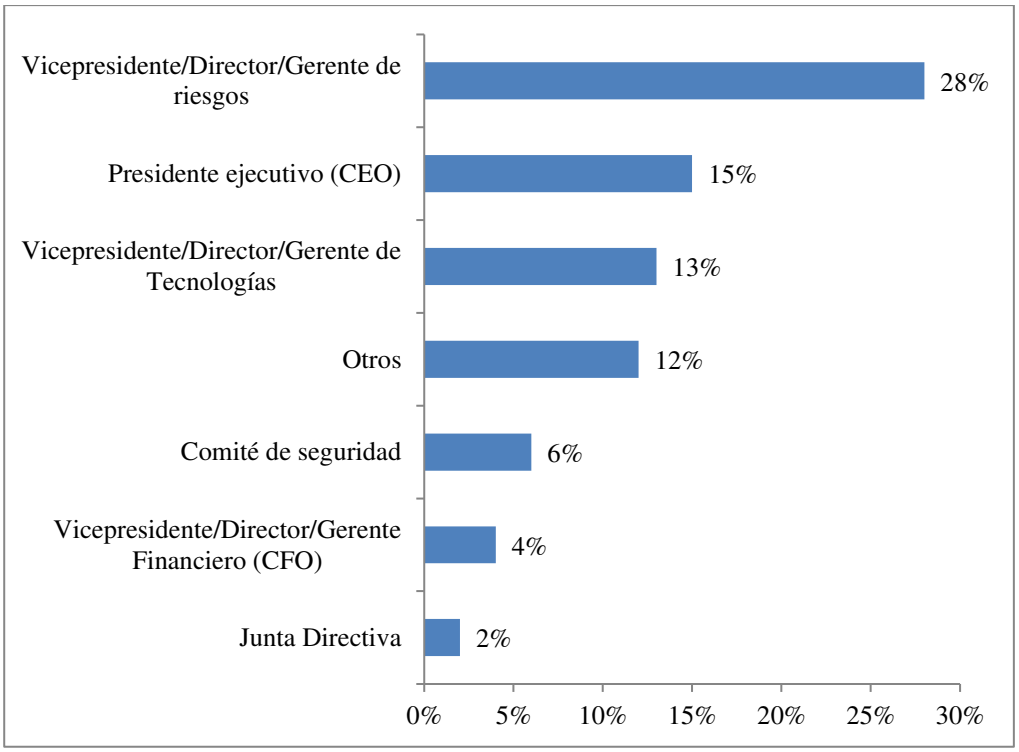


Figura 9. Unidades a quien reporta el CISO
(Deloitte, 2017)

Las áreas o funciones en las cuales se encuentran bajo la responsabilidad del CISO pueden ser diversas, donde el 74% de encuestados se encargan del Gobierno de la Seguridad de la Información, encargados de desarrollar y aplicar políticas, normas y estándares, el 72% de los CISO se encargan del Monitoreo de la Seguridad de la Información, orientados a determinar el cumplimiento en base a indicadores, métricas y elaboración de reportes. En la Figura 10, se puede visualizar con mayor detalle esta información.

[1] CISO. Chief Information Security Officer

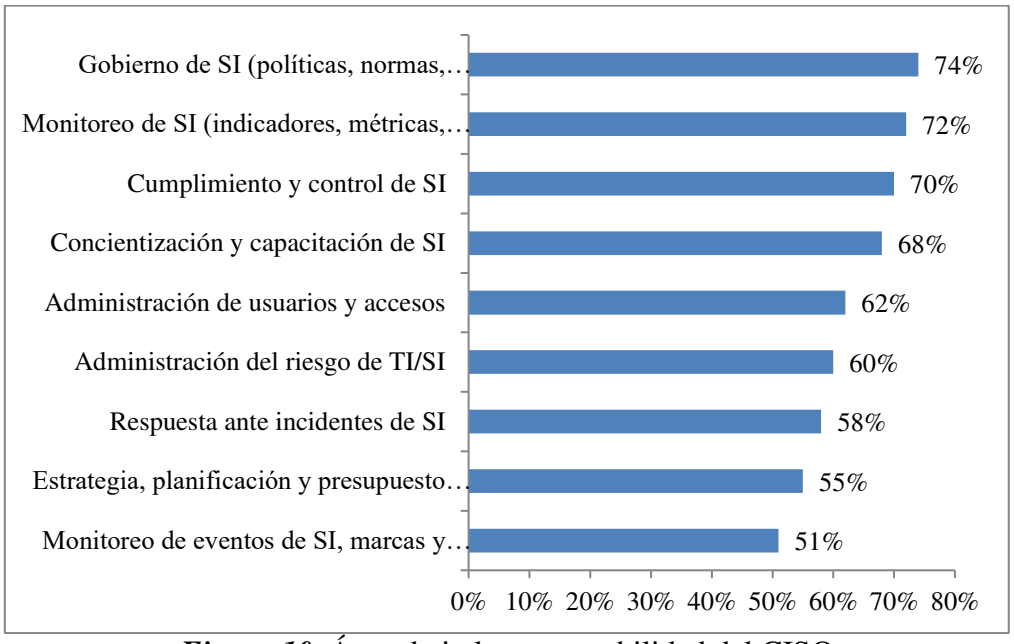


Figura 10. Áreas bajo la responsabilidad del CISO
(Deloitte, 2017)

En la Figura 11, se puede visualizar el enfoque del monitoreo de la seguridad de la Información, en donde el 36% de las empresas encuestadas no cuenta con un enfoque de monitoreo referente a seguridad de la información, el 30% cuenta con métricas de Seguridad de la Información, el 19% cuentan con un esquema de medición mediante métricas operacionales, y apenas el 19% han establecido indicadores clave del proceso e indicadores claves de riesgo referentes a seguridad de la información.

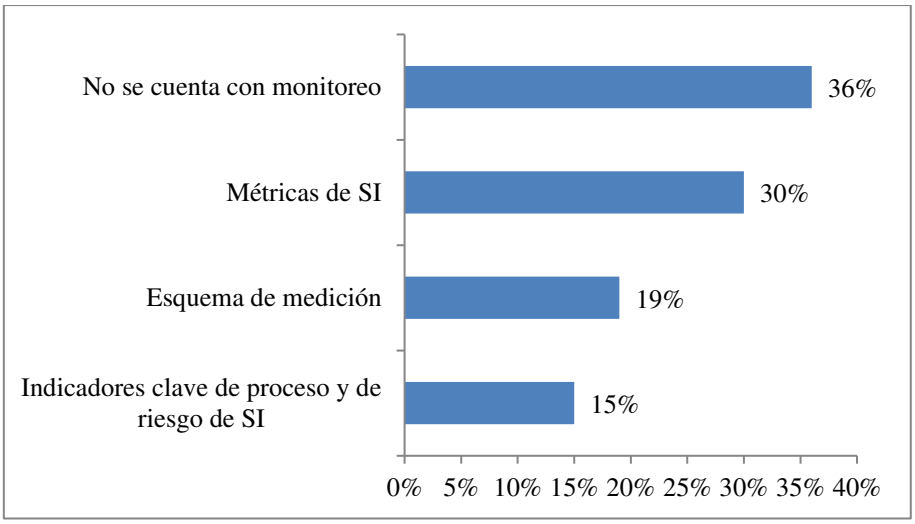


Figura 11. Monitoreo de la Seguridad de la Información
(Deloitte, 2017)

Los procesos o tecnologías implementadas en las empresas encuestadas se detallan en la Figura 12, donde se indica que el 53% cuentan con procesos operativos que pueden servir para monitorear los riesgos, el 42% cuentan con procesos específicos y tecnología implementada para monitoreo, el 30% cuenta con revisores de terceros y el 15% no cuentan con herramientas ni procesos.

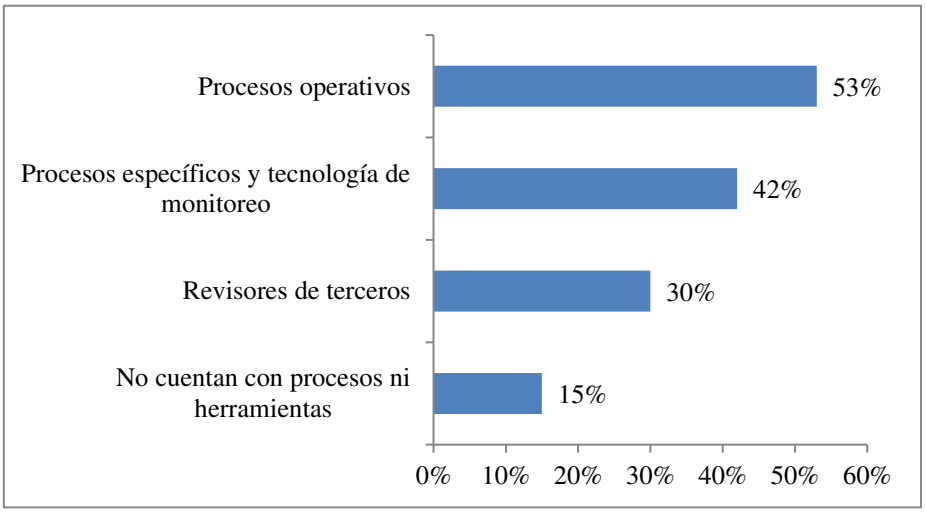


Figura 12. Procesos y/o tecnologías de riesgo
(Deloitte, 2017)

La importancia de contar con un SOC es importante para la gestión de la seguridad de la información, ya que este centro de operaciones consta con las herramientas necesarias y el personal calificado para gestionar la seguridad de la información. De acuerdo a la Figura 13 el 60% de las instituciones que participaron en el estudio, no disponen de un SOC, el 21% si disponen, pero el 19% piensan implementar uno para el 2019.

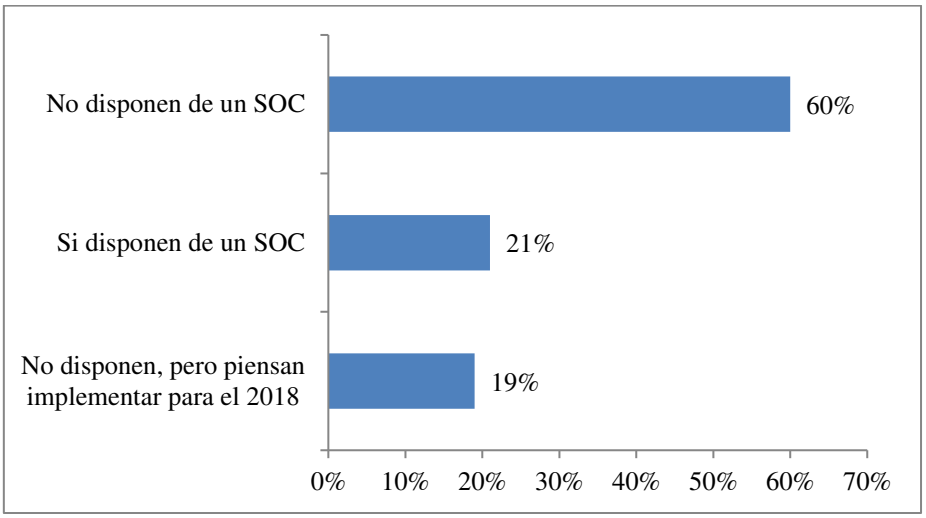


Figura 13. Disposición de un SOC
(Deloitte, 2017)

En resumen, el estudio muestra también las observaciones de auditoría interna y externa que las empresas participantes en el estudio han recibido con el fin de receptar las mejores recomendaciones y fortalecer la gestión de la seguridad de la información en los últimos 12 meses. Dicha información se puede mostrar en la Figura 14.

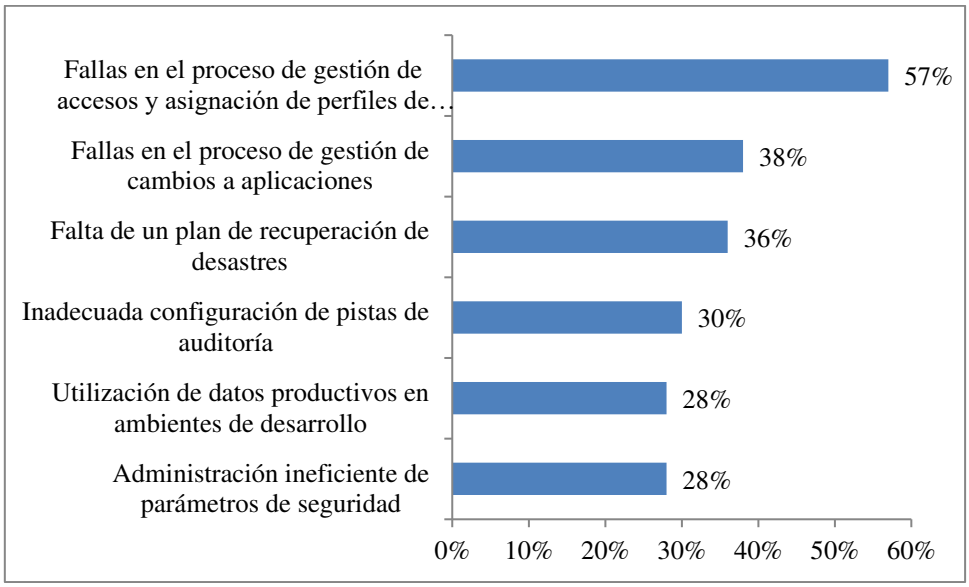


Figura 14. Observaciones de auditoría
(Deloitte, 2017)

4.1.4 Políticas internas en el sector académico

Como Evidencia O-10 recopilada mediante el instrumento de investigación Estado de las Tecnologías de la Información y Comunicación en las Universidades del Ecuador del 2017 realizado por CEDIA, se muestran la siguiente información.

En el 2017, la Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia (CEDIA), denominada como la Red Nacional de Investigación y Educación del Ecuador emite su informe en el 2017 sobre el Estado de las Tecnologías de la Información y Comunicación de las Universidades ecuatorianas, en donde se analiza el estado de la Seguridad de TIC en estas universidades.

De un universo de 60 universidades públicas y privadas, donde el tamaño muestral fue de 37, se analizan los siguientes datos.

Referente a las políticas de seguridad TIC, necesarias en las instituciones para poder actuar de forma oportuna basados en buenas prácticas y normas técnicas, el 32% de las universidades no cuentan con dichas políticas, el 60% cuentan con políticas de manera parcial y apenas el 8% tienen políticas de seguridad formalizadas, tal y como se muestra en la Figura 15.

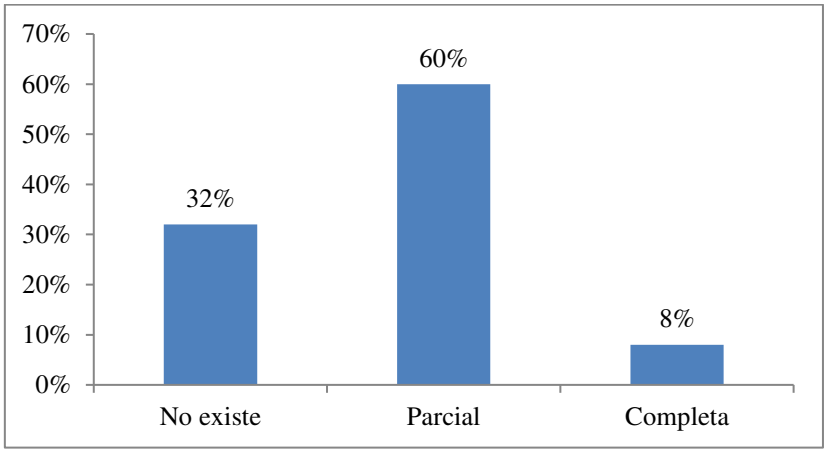


Figura 15. Políticas de seguridad en Universidades
Fuente: (CEDIA, 2017)

De las universidades encuestadas, el 51% de las instituciones indican que el responsable de la seguridad de la información forma parte de la estructura de TI, el 6% no es parte de TI y un 43% indicó que no cuenta con un responsable de seguridad de la información. Ver Figura 16.

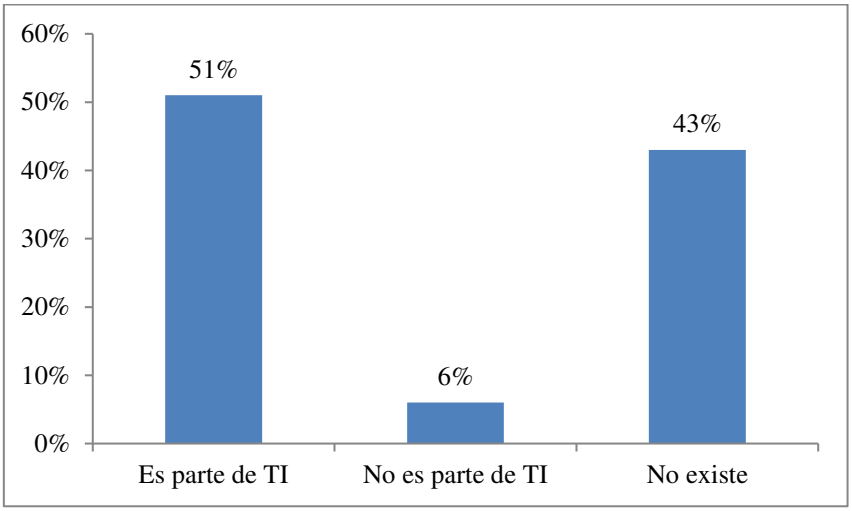


Figura 16. Responsable de la seguridad de la información en Universidades
Fuente: (CEDIA, 2017)

La Figura 17 indica que el 59% de las universidades encuestadas no realizan auditorías de seguridad de la información, el 27% realiza auditorías específicas y el 14% realiza auditorías específicas y además periódicas.

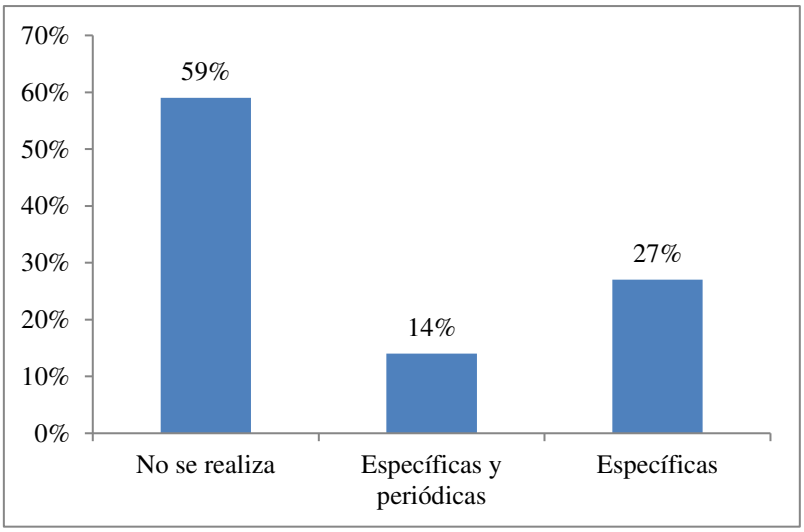


Figura 17. Auditorías de seguridad de la información en Universidades
Fuente: (CEDIA, 2017)

Los planes de contingencia son importantes para determinar las acciones que se deben realizar ante amenazas, sin embargo, solo el 16% de los encuestados cuentan con un plan de

contingencia aprobado y difundido, 30% tiene un plan aprobado y el 54% no cuenta con un plan de contingencia. Ver Figura 18.

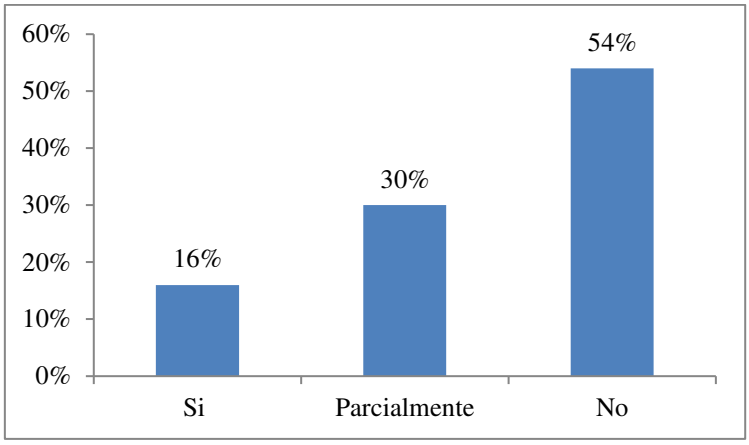


Figura 18. Planes de contingencia en Universidades
Fuente: (CEDIA, 2017)

Así mismo, las instituciones deben contar con un plan de continuidad que permita mantener y garantizar la prestación de servicios TIC, y ante ello, en la Figura 19 se muestra que solo el 27% cuenta con un plan de continuidad aprobado, el 3% tienen un plan solo aprobado, el 3% lo difundido y aprobado, y el 67% no cuenta con este documento.

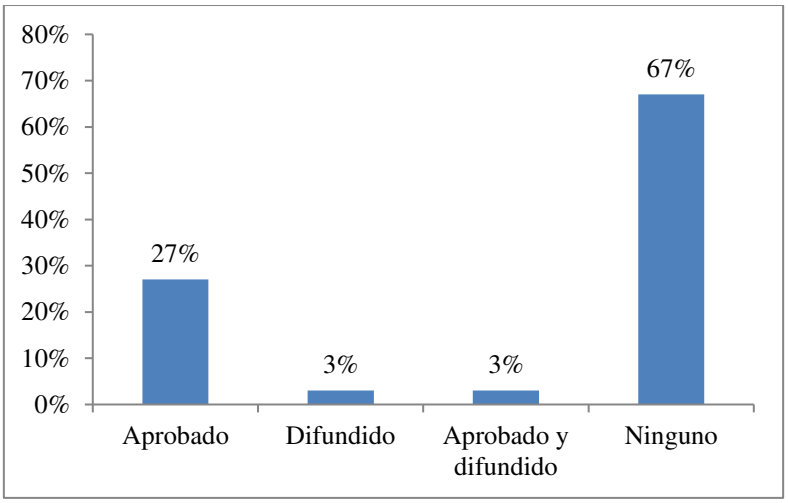


Figura 19. Planes de continuidad en Universidades
Fuente: (CEDIA, 2017)

4.1.5 Incidentes y vulnerabilidades

Esta información se muestra como Evidencia O-03 recopilada mediante el instrumento de investigación LBCE-IIC-03 (Ver Anexo C).

4.1.5.1 Incidentes

Según (ARCOTEL, 2018), Ecuador ha tenido varias clases de incidentes informáticos, con peligro de comprometer las operaciones de un sistema y de amenazar la seguridad de la información y que han puesto en riesgo su confidencialidad, integridad o disponibilidad.

Los principales incidentes registrados en Ecuador se pueden detallar en la Tabla 5.

Tabla 5
Incidentes registrados en el Ecuador desde 2017

Nro.	Incidente
1	Blacklisted
2	Bruteforce
3	CC_Server
4	Compromised_website
5	Drones_Botnet
6	Sandbox_URL
7	Sinkhole (varios tipos)
8	Spam

Fuente: (ARCOTEL, 2018)

Desde enero del 2017, ha existido un gran número de incidentes. En el 2018, hasta el mes de junio se han contabilizado 742512 incidentes. En la Figura 20 se puede observar el número de incidentes ocurridos desde enero del 2017 hasta junio del 2018.

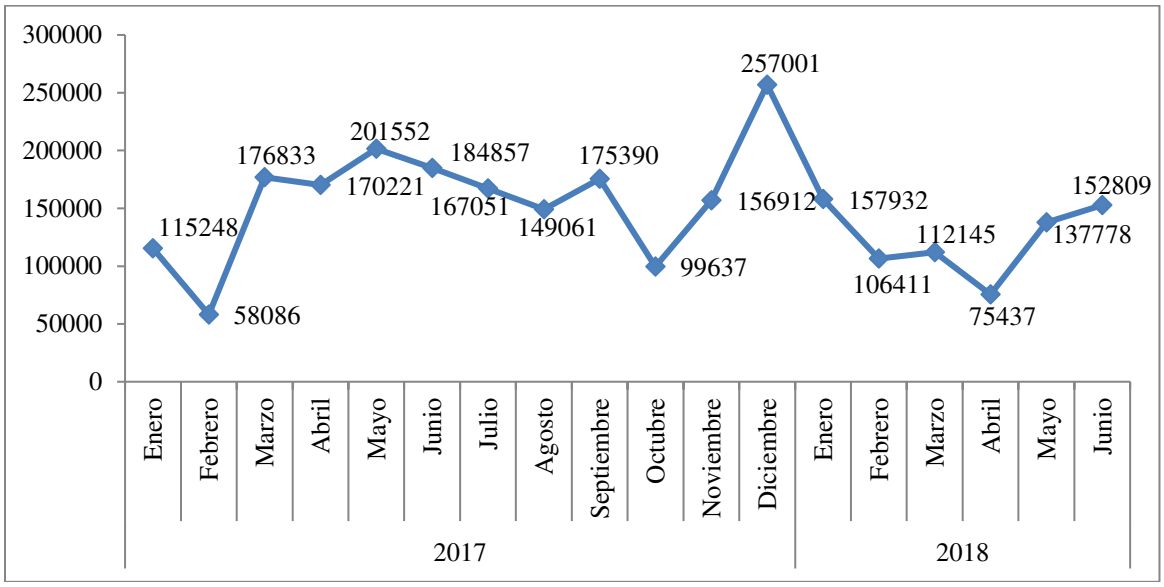


Figura 20. Incidentes informáticos contabilizados en el Ecuador
Fuente: (ARCOTEL, 2018)

4.1.5.2 Vulnerabilidades

En Ecuador, los principales tipos de vulnerabilidades detectados desde enero 2017 a julio 2018 de acuerdo a (ARCOTEL, 2018) se pueden visualizar en la Tabla 6.

Tabla 6
Amenazas registradas en el Ecuador desde 2017

Nro.	Vulnerabilidad	Nro.	Vulnerabilidad
1	Accesible_RDP	**17**	Open_Netbios
2	Cisco_SmartInstall	**18**	Open_NTP_monitor
3	CWMP	**19**	Open_NTP_version
4	DNS_Open_Resolver	**20**	Open_Portmapper
5	Freak_SSL	**21**	Open_Proxy
6	Isakmp	**22**	Open_Qotd
7	LDAP	**23**	Open_Redis
8	mDNS	**24**	Open_SMB
9	NAT_PMP	**25**	Open_SNMP
10	Netis_Router	**26**	Open_SQL_Server_Resl
11	Open_Chargen	**27**	Open_SSDP
12	Open_DB2	**28**	Open_Telnet
13	Open_Elasticsearch	**29**	Open_TFTP
14	Open_IPMI	**30**	Open_VNC
15	Open_Memcached	**31**	Poodle_SSLv3
16	Open_MongoDB	**32**	XDMCP

Fuente: (ARCOTEL, 2018)

Hasta junio del 2018, se han detectado 6169255 vulnerabilidades por la (ARCOTEL, 2018). En la Figura 21 se puede visualizar las vulnerabilidades detectadas en el Ecuador desde el 2017 hasta junio del 2018 contabilizadas por mes.

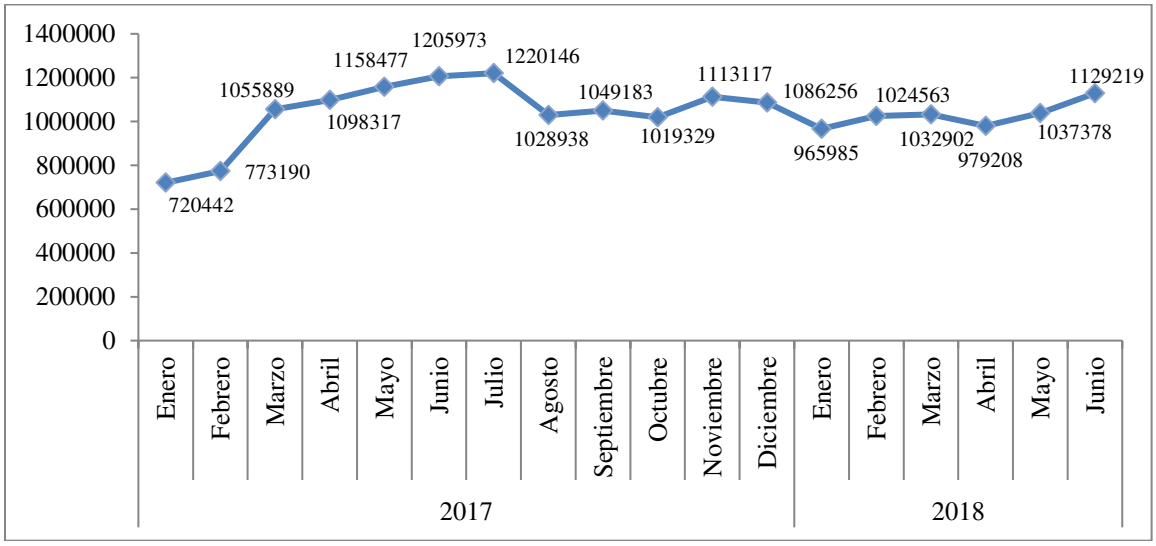


Figura 21. Vulnerabilidades contabilizadas en el Ecuador
Fuente: (ARCOTEL, 2018)

4.2 Estado del marco penal

En Ecuador, con la aprobación de la Ley de Comercio Electrónico publicada mediante Registro Oficial 557 del 17 de abril del 2002, existieron reformas al Código Penal, originando los delitos informáticos en el país. Los delitos que se definieron en el 2002 son: Acceso no autorizado, falsificación informática, fraude informático, daños informáticos, violaciones al derecho a la intimidad. En agosto del 2014, con la aprobación del Código Orgánico Integral Penal (COIP) en agosto del 2014, se tipificaron delitos que tienen relación con el acoso a través de medios digitales hacia niños niñas y adolescentes (grooming[2]), posesión de

[2] Grooming. Es el conjunto de estrategias que una persona adulta realiza para ganarse la confianza de un niño, niña o adolescente, a través del uso de las tecnologías de la comunicación información, con el propósito de abusar o explotar sexualmente de él o ella. El adulto suele crear un perfil falso en una red social, foro, sala de chat u otro, se hace pasar por un chico o una chica y entablan una relación con el niño o niña con la intención de acosarlo.

pornografía infantil, permitiendo abarcar los tipos de delitos informáticos en Ecuador. (Acurio, 2017)

De acuerdo a (Ron, Fuertes, Bonilla, Toulkeridis, & Diaz, 2018), los delitos informáticos referentes a Ciberseguridad definidos en el COIP son los detallados en la Tabla 7.

Tabla 7
Delitos informáticos referentes a Ciberseguridad estipulados en el COIP

Código	Descripción
Art. 173	Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos
Art. 174	Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos
Art. 186	Estafa[3]
Art. 190	Apropiación fraudulenta por medios Electrónicos
Art. 229	Revelación ilegal de base de datos
Art. 230	Interceptación ilegal de datos
Art. 231	Transferencia electrónica de activo patrimonial
Art. 232	Ataque a la integridad de sistemas informáticos
Art. 233	Delitos contra la información pública reservada legalmente
Art. 234	Acceso no consentido a un sistema informático, telemático o de telecomunicaciones

Fuente: (Ron, Fuertes, Bonilla, Toulkeridis, & Diaz, 2018)

Como Evidencia O-04 recopilada mediante el instrumento de investigación LBCE-IIC-04 (Ver Anexo C), se muestran la siguiente información facilitada por la Fiscalía General del Estado, desde agosto el 2014 que entró en vigencia el COIP, hasta abril del 2018, se ha

[3] De acuerdo al COIP, el delito denominado Estafa solo determina en el numeral 2 como delito informático, ya que se hace referencia al fraude mediante el uso de dispositivos electrónicos.

contabilizado un total de 5955 delitos informáticos. Cabe señalar que no se considera en esta estadística al delito de Estafa, ya que posee muchos numerales que determinan los casos de este delito, pero solo en uno de ellos interviene las TIC, lo que deriva en un dato inexacto.

En la Tabla 8, se puede visualizar los delitos informáticos ocurridos desde agosto del 2014, cuando entró en vigencia el COIP, hasta abril del 2018.

Tabla 8

Número de delitos informáticos desde agosto del 2014 hasta abril del 2018

Art. COIP	DELITOS	2014	2015	2016	2017	2018	TOTAL
173	CONTACTO CON FINALIDAD SEXUAL CON MENORES DE DIECIOCHO AÑOS POR MEDIOS ELECTRÓNICOS	21	80	108	160	81	**450**
174	OFERTA DE SERVICIOS SEXUALES CON MENORES DE DIECIOCHO AÑOS POR MEDIOS ELECTRÓNICOS	0	6	9	12	7	**34**
190	APROPIACIÓN FRAUDULENTA POR MEDIOS ELECTRÓNICOS	507	1283	1049	966	535	**4340**
229	REVELACIÓN ILEGAL DE BASE DE DATOS	30	24	24	22	21	**121**
230	INTERCEPTACIÓN ILEGAL DE DATOS	38	55	83	64	15	**255**
231	TRANSFERENCIA ELECTRÓNICA DE ACTIVO PATRIMONIAL	17	60	43	58	15	**193**
232	ATAQUE A LA INTEGRIDAD DE SISTEMAS INFORMÁTICOS	49	78	76	88	50	**341**
233	DELITOS CONTRA LA INFORMACIÓN PÚBLICA RESERVADA LEGALMENTE	6	5	3	15	6	**35**
234	ACCESO NO CONSENTIDO A UN SISTEMA INFORMÁTICO, TELEMÁTICO O DE TELECOMUNICACIONES	54	142	145	221	108	**670**
TOTAL		701	1647	1423	1434	750	**5955**

Fuente: (FGE, 2018)

4.2.1 Análisis del Artículo 173, "Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos"

Según el COIP, se sancionará con pena privativa de libertad de uno a tres años a quien *"... a través de un medio electrónico o telemático proponga concertar un encuentro con una persona menor de dieciocho años, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento con finalidad sexual o erótica..."*. (Asamblea Nacional, 2014)

Así mismo, se sancionará con pena privativa de libertad de tres a cinco años a quien *"...suplantando la identidad de un tercero o mediante el uso de una identidad falsa por medios electrónicos o telemáticos, establezca comunicaciones de contenido sexual o erótico con una persona menor de dieciocho años o con discapacidad..."* (Asamblea Nacional, 2014)

Desde agosto del 2014, hasta abril del 2018, se muestra que la provincia con mayor número de denuncias sobre el Artículo 173 del COIP es Guayas con 122 denuncias, seguido de Pichincha con 73 y Manabí con 54, tal y como se muestra en la Figura 22.

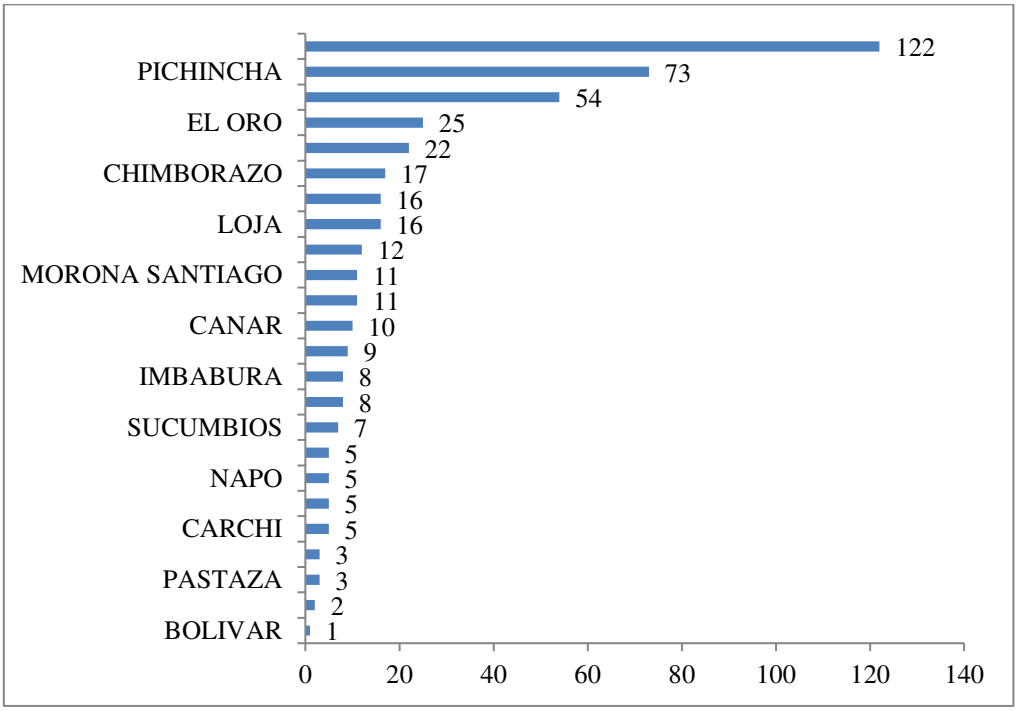


Figura 22. Número de denuncias sobre el Artículo 173 del COIP por provincias
Fuente: (FGE, 2018)

Además en la Figura 23, se visualiza que en el 2017 se han contabilizado un mayor número de denuncias sobre este delito, A abril del 2018 ya existen 81 denuncias.

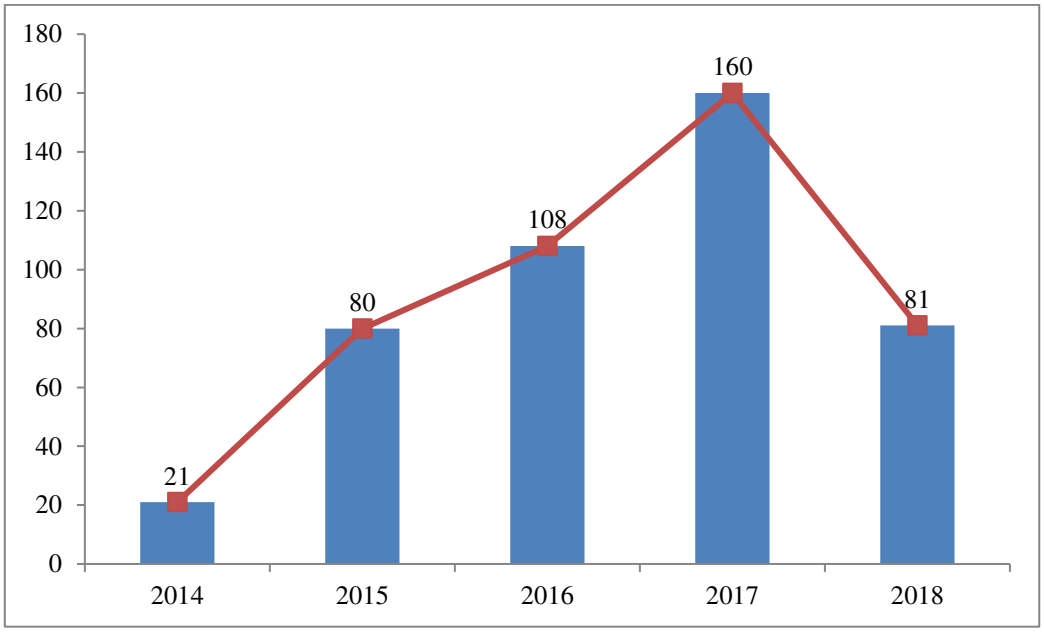


Figura 23. Número de denuncias sobre el Artículo 173 del COIP por años
Fuente: (FGE, 2018)

4.2.2 Análisis del Artículo 174, "Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos"

Se sancionará con pena privativa de libertad de siete a diez años a quienes "*utilicen o faciliten el correo electrónico, chat, mensajería instantánea, redes sociales, blogs, fotoblogs, juegos en red o cualquier otro medio electrónico o telemático para ofrecer servicios sexuales con menores de dieciocho años de edad*". (Asamblea Nacional, 2014)

Por provincias, Guayas posee el mayor número de casos sobre este delito con 9 denuncias, seguido de Manabí y Pichincha, de acuerdo a la Figura 24.

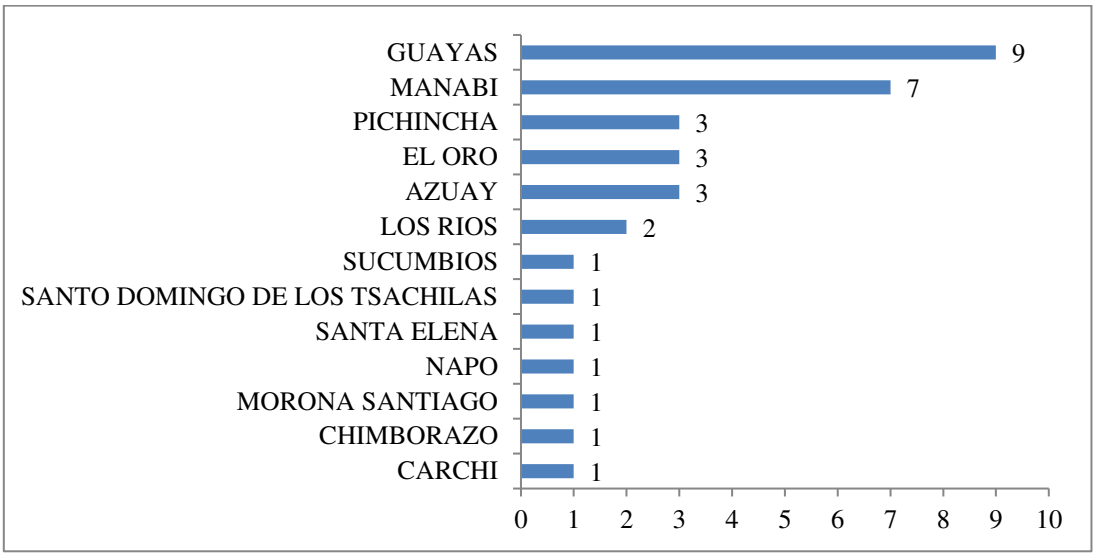


Figura 24. Número de denuncias sobre el Artículo 174 del COIP por provincias
Fuente: (FGE, 2018)

La Figura 25 indica el número de denuncias sobre el Artículo 174 del COIP por años, donde se muestra que en el 2017 se han realizado un mayor número de denuncias referentes a este delito.

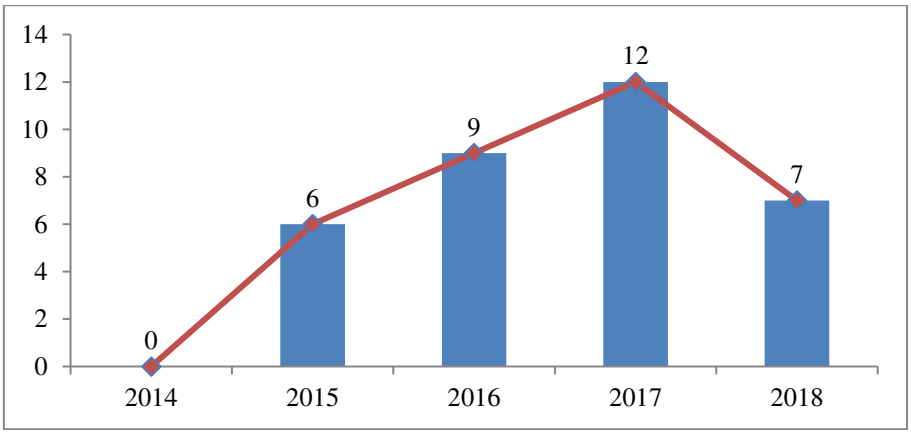


Figura 25. Número de denuncias sobre el Artículo 174 del COIP por años
Fuente: (FGE, 2018)

4.2.3 Análisis del Artículo 190, "Apropiación fraudulenta por medios electrónicos"

Se aplicará la sanción de privación de libertad de uno a tres años a quien *"...utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra*

persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones…". (Asamblea Nacional, 2014)

Se impondrá la misma sanción a quien "*...comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes*". (Asamblea Nacional, 2014)

En la Figura 26, se muestra el número de denuncias referentes a la apropiación fraudulenta por medios electrónicos, desde el 2014 hasta el 2018, donde Guayas posee el mayor número de denuncias con 1431, seguidos de Pichincha con 1192 y El Oro con 320.

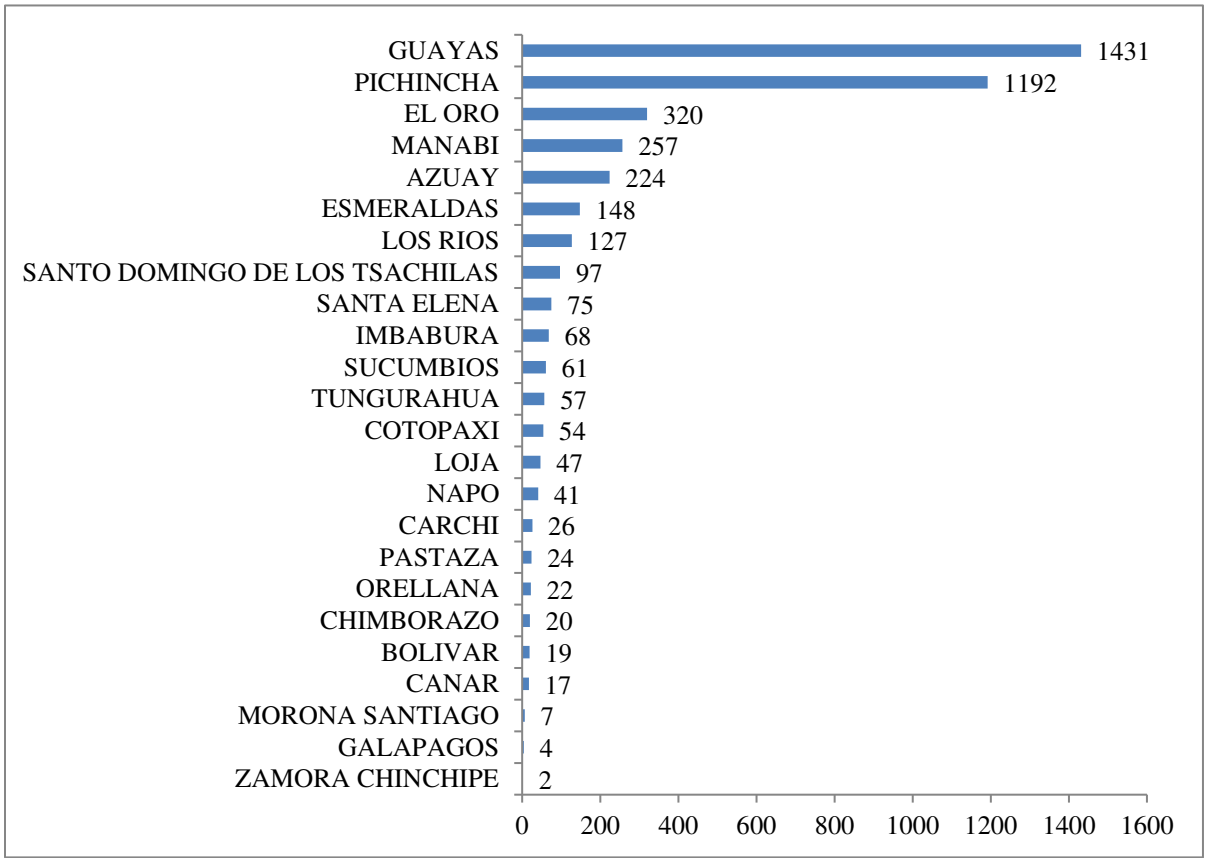


Figura 26. Número de denuncias sobre el Artículo 190 del COIP por provincias
Fuente: (FGE, 2018)

Además, se observa que el mayor número de denuncias se realizaron en el 2015, con un total de 1 283 casos, tal y como se muestra en la Figura 27.

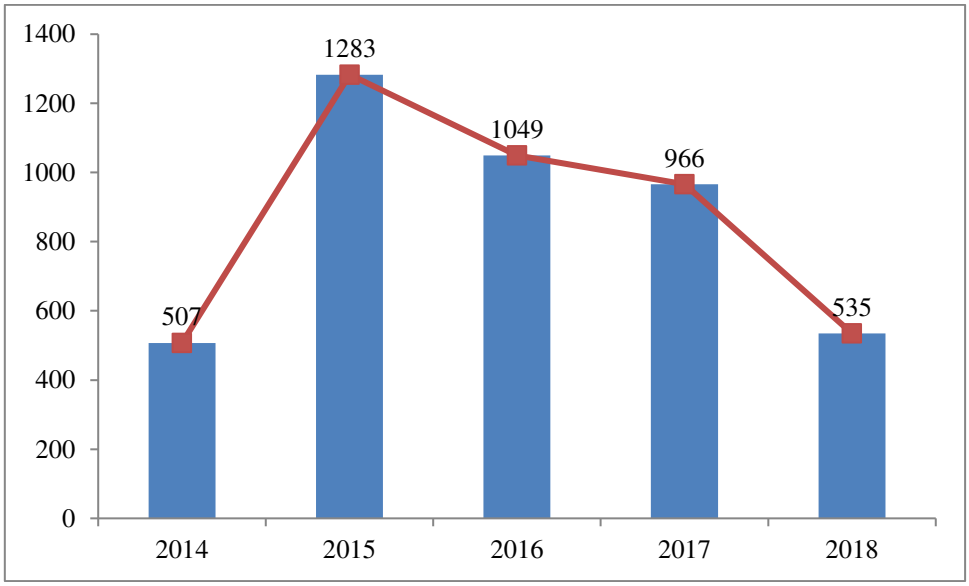


Figura 27. Número de denuncias sobre el Artículo 190 del COIP por años
Fuente: (FGE, 2018)

4.2.4 Análisis del Artículo 229, "Revelación ilegal de base de datos"

Se sancionará con la pena privativa de libertad de uno a tres años, a quien la persona que "*... en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas…*". (Asamblea Nacional, 2014)

Así mismo, tendrá une pena privativa de tres a cinco años "*…si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas…*". (Asamblea Nacional, 2014)

En las Figura 28 y Figura 29 se muestran las estadísticas sobre la revelación ilegal de bases de datos, por provincias y por años desde agosto del 2014 hasta abril del 2018.

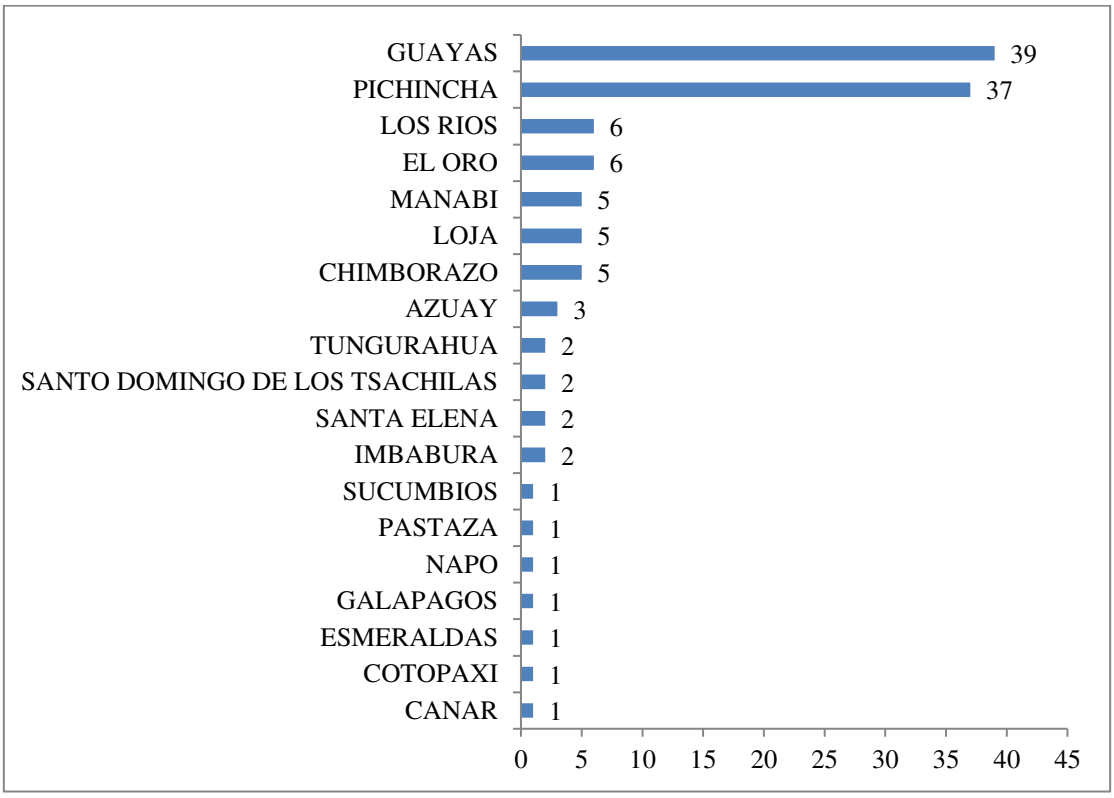


Figura 28. Número de denuncias sobre el Artículo 229 del COIP por provincias
Fuente: (FGE, 2018)

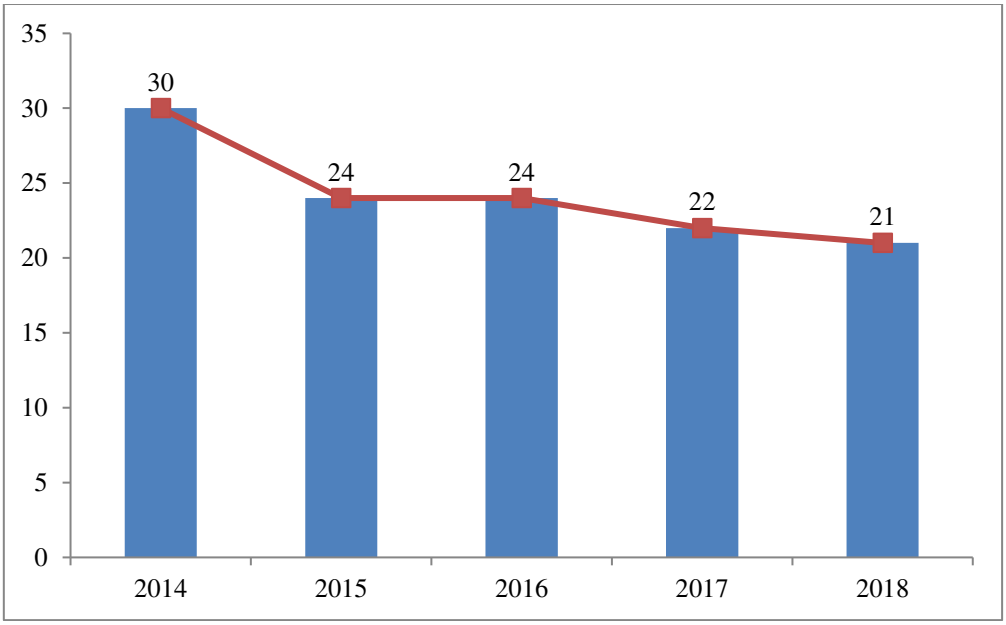


Figura 29. Número de denuncias sobre el Artículo 229 del COIP por años
Fuente: (FGE, 2018)

4.2.5 Análisis del Artículo 230, "Interceptación ilegal de datos"

Para el delito de interceptación de datos, la sanción correspondiente es la privación de libertad de tres a cinco años, en los siguientes casos:

"1. La persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.

2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.

3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.

4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior." (Asamblea Nacional, 2014)

Pichincha figura como la provincia con más casos de interceptación ilegal de datos, con un total de 133 en cuatro años, seguido por Guayas con 46 y Santo Domingo de los Tsáchilas con 14, tal y como se muestra en la Figura 30.

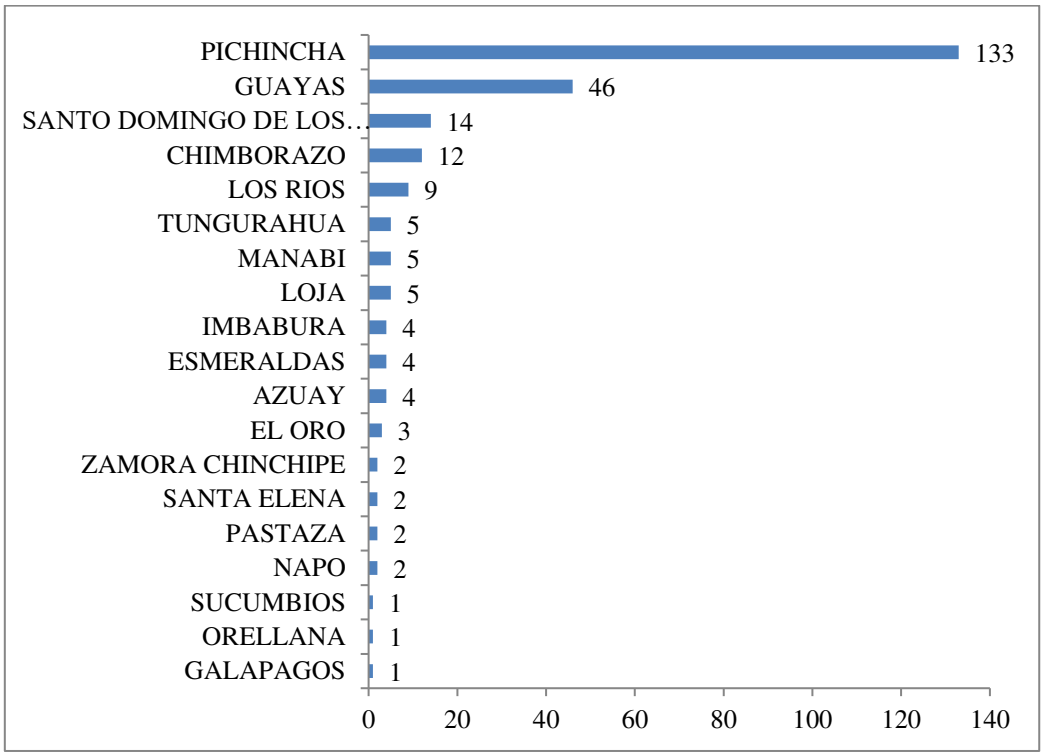


Figura 30. Número de denuncias sobre el Artículo 230 del COIP por provincias
Fuente: (FGE, 2018)

En el 2016 se han contabilizado 83 denuncias sobre interceptación ilegal de datos, hasta abril del 2018 existen 15 denuncias por este delito. La información se la puede visualizar Figura 31.

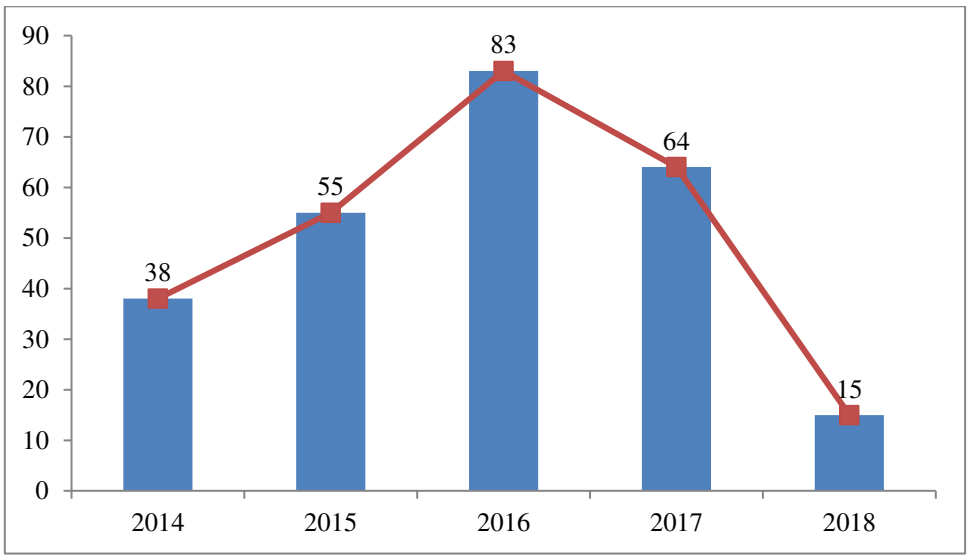


Figura 31. Número de denuncias sobre el Artículo 230 del COIP por años
Fuente: (FGE, 2018)

4.2.6 Análisis del Artículo 231, "Transferencia electrónica de activo patrimonial"

La transferencia electrónica de activo patrimonial es sancionada con pena privativa de libertad de tres a cinco años a quien, "…con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero…".

De igual manera a quien "… facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona.".

Desde agosto del 2014 con la aprobación del COIP, se han contabilizado 54 denuncias en la Fiscalía General del Estado referente a este delito en la provincia del Guayas, seguido por Pichincha con 50 denuncias y Manabí con 22 denuncias, tal y como se muestra en la Figura 32.

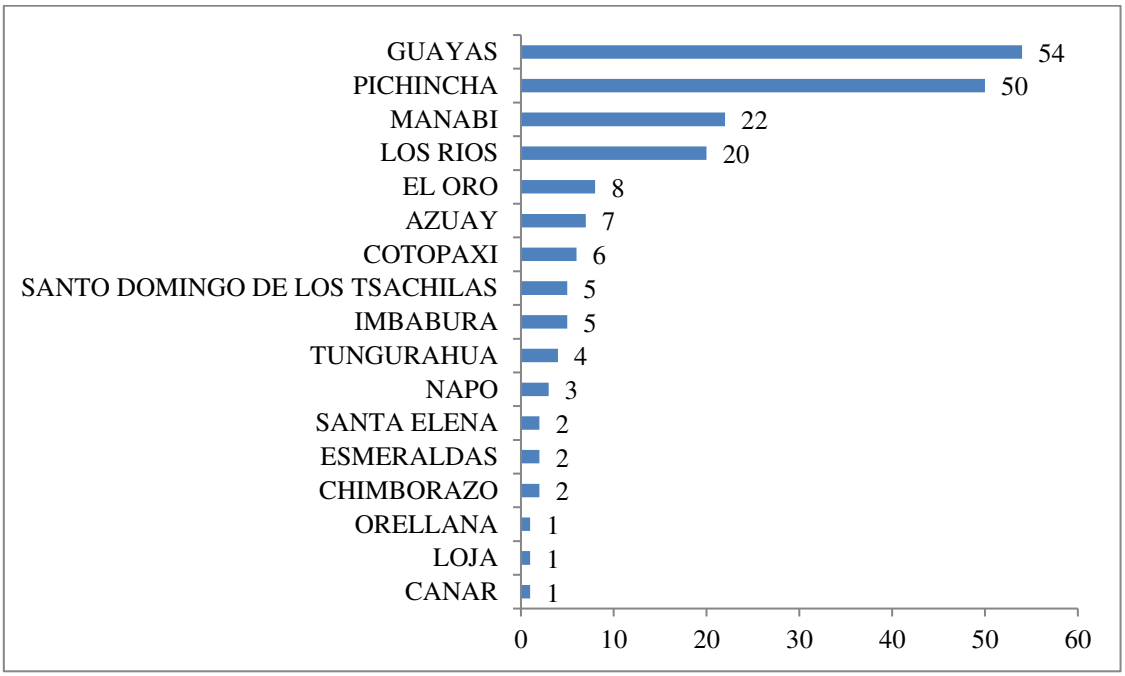


Figura 32. Número de denuncias sobre el Artículo 231 del COIP por provincias
Fuente: (FGE, 2018)

En el 2015 y 2017 se han contabilizado la mayoría de denuncias con 60 y 58 respectivamente. A abril del 2018 existen 15 denuncias sobre transferencia electrónica de uso patrimonial, tal y como se muestra en la Figura 33.

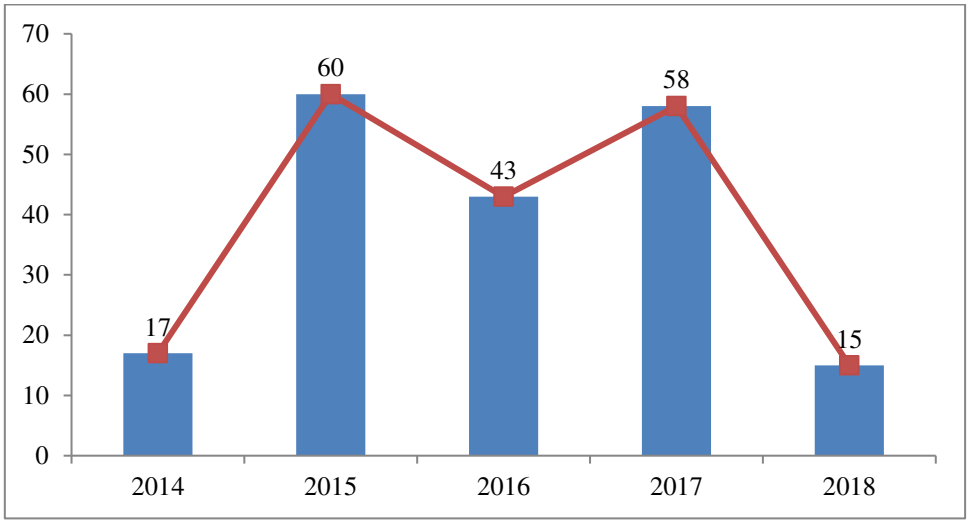


Figura 33. Número de denuncias sobre el Artículo 231 del COIP por años
Fuente: (FGE, 2018)

4.2.7 Análisis del Artículo 232, "Ataque a la integridad de sistemas informáticos"

La sanción para este delito es pena privativa de libertad de tres a cinco años para quien *"…destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen…*".

De igual manera para la persona que:

"1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.

2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.

Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad".

La provincia del Guayas hasta abril del 2018 ha contabilizado 95 denuncias sobre ataques a la integridad de la información, seguido de Pichincha con 93 y Bolívar con 27, tal y como se muestra en la Figura 34.

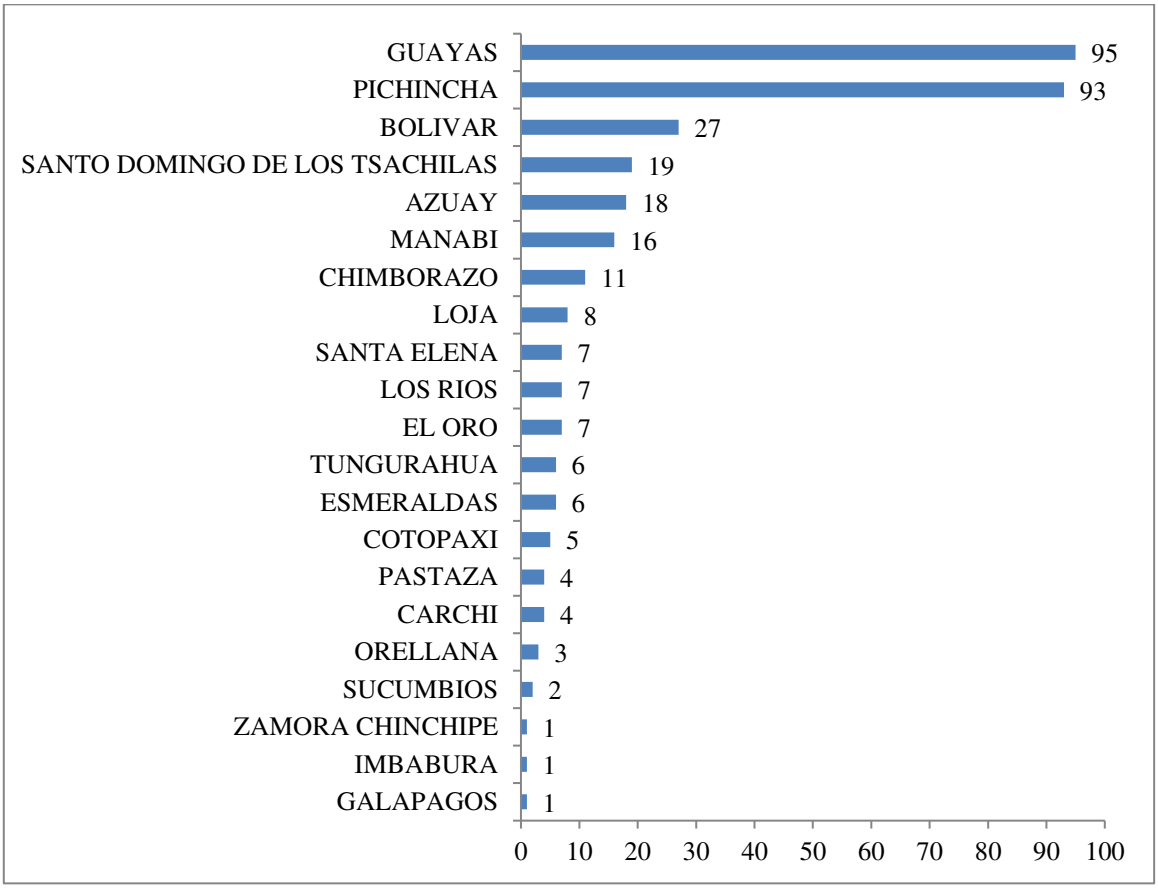


Figura 34. Número de denuncias sobre el Artículo 232 del COIP por provincias
Fuente: (FGE, 2018)

En el 2017 se han contabilizado la mayor cantidad de denuncias sobre este delito, con 88 denuncias, tal y como se muestra en la Figura 35.

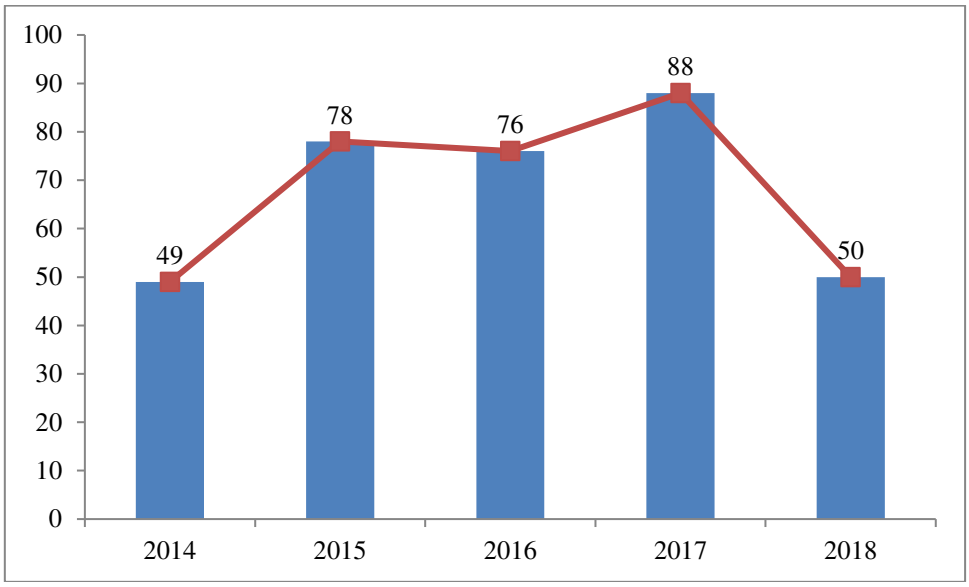


Figura 35. Número de denuncias sobre el Artículo 232 del COIP por años
Fuente: (FGE, 2018)

4.2.8 Análisis del Artículo 233, "Delitos contra la información pública reservada legalmente"

Se privará de libertad de cinco a siete años a quien *"...destruya o inutilice información clasificada de conformidad con la Ley..."*, así mismo al servidor público que "*...utilizando cualquier medio electrónico o informático, obtenga este tipo de información…*", se sancionará con privación de libertad de tres a cinco años. (Asamblea Nacional, 2014)

En caso de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, se privará de pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses al *"...servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información*", siempre que no se configure otra infracción de mayor gravedad. (Asamblea Nacional, 2014)

Pichincha figura como la provincia con mayor número de denuncias desde el 2014 con 18, seguido de Manabí con 6 y Guayas con 4, tal y como se menciona en la Figura 36.

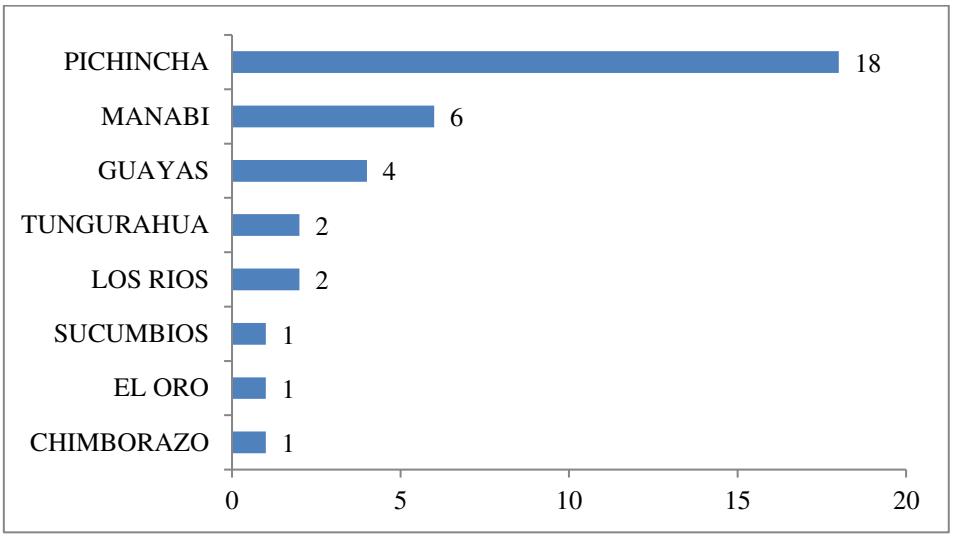


Figura 36. Número de denuncias sobre el Artículo 233 del COIP por provincias
Fuente: (FGE, 2018)

En la Figura 37, indica que en el 2017 se han recibido 15 denuncias en el 2017, y hasta abril del 2018, se han receptado 6 denuncias, según (FGE, 2018).

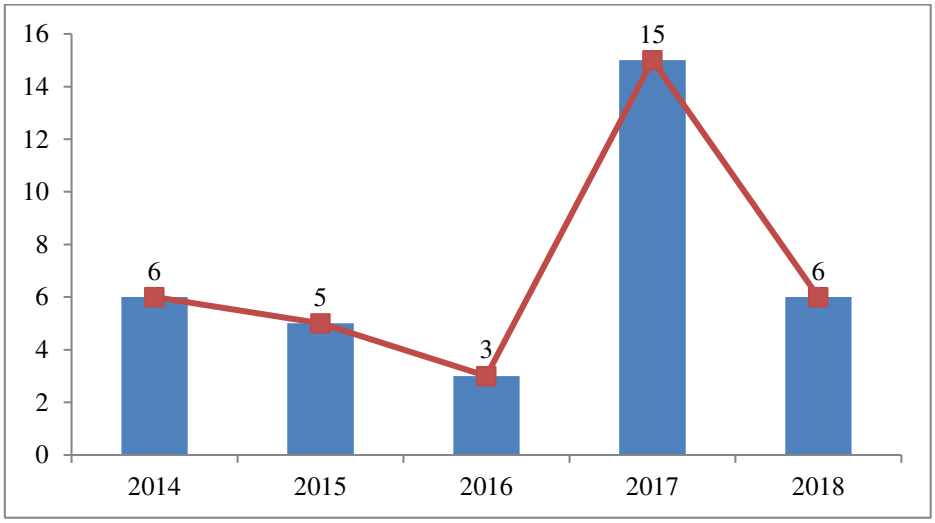


Figura 37. Número de denuncias sobre el Artículo 233 del COIP por años
Fuente: (FGE, 2018)

4.2.9 Análisis del Artículo 234, "Acceso no consentido a un sistema informático, telemático o de telecomunicaciones"

Para la presente sanción, se aplicará una pena de privación de libertad de tres a cinco años, a quien *"...sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad*

de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos…"

Desde el 2014, en Pichincha se ha visto mayor incidencia de denuncias sobre el acceso no so consentido a un sistema informático, telemático o de telecomunicaciones con 247 denuncias, seguido por Guayas con 244 y Azuay con 52, tal y como se muestra en la Figura 38.

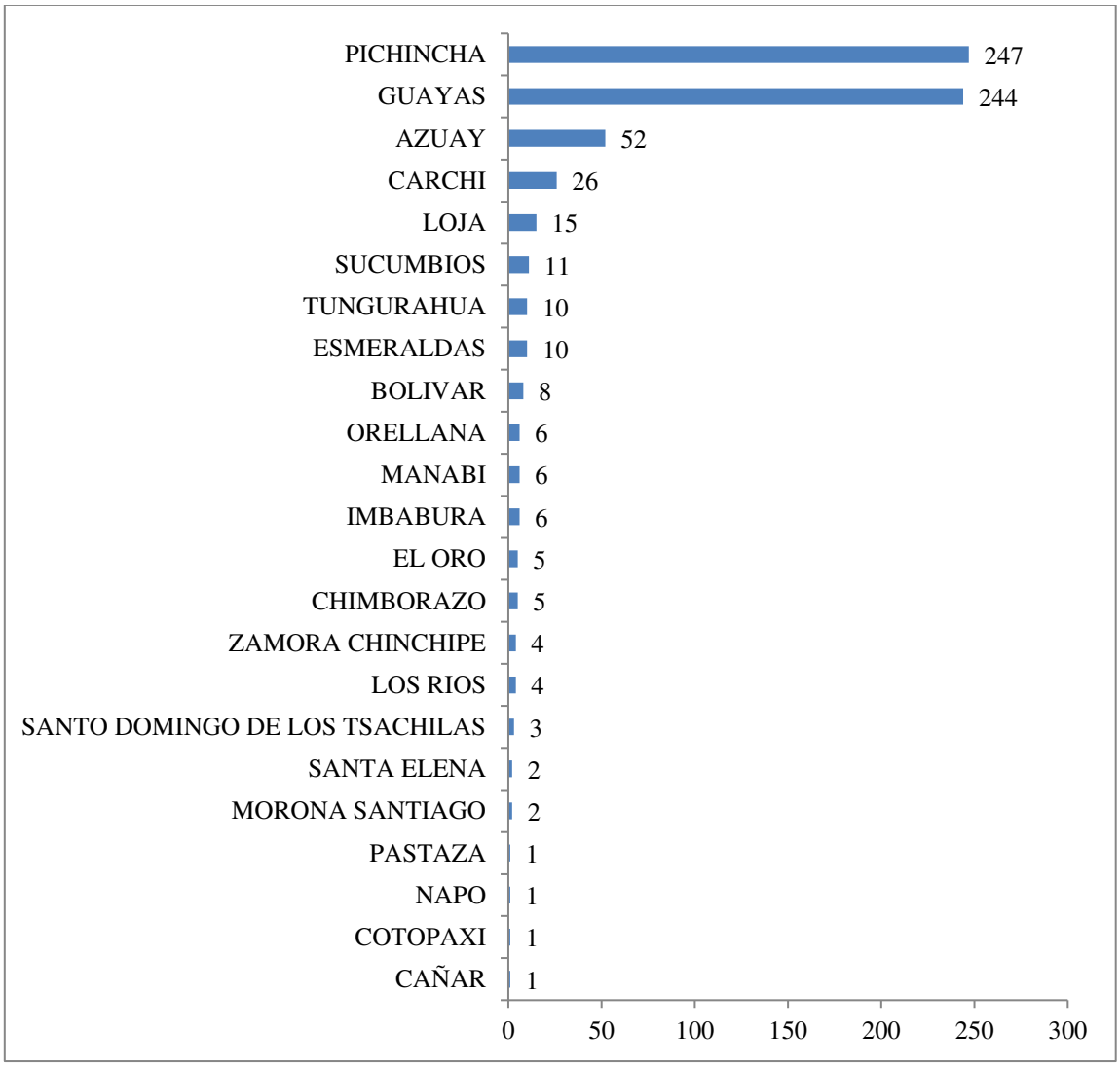


Figura 38. Número de denuncias sobre el Artículo 234 del COIP por provincias
Fuente: (FGE, 2018)

De igual manera, en la Figura 39 que en el 2017 se han receptado un mayor número de denuncias, con 221 casos. A abril del 2018 se contabiliza 108 casos de denuncias sobre acceso no so consentido a un sistema informático, telemático o de telecomunicaciones.

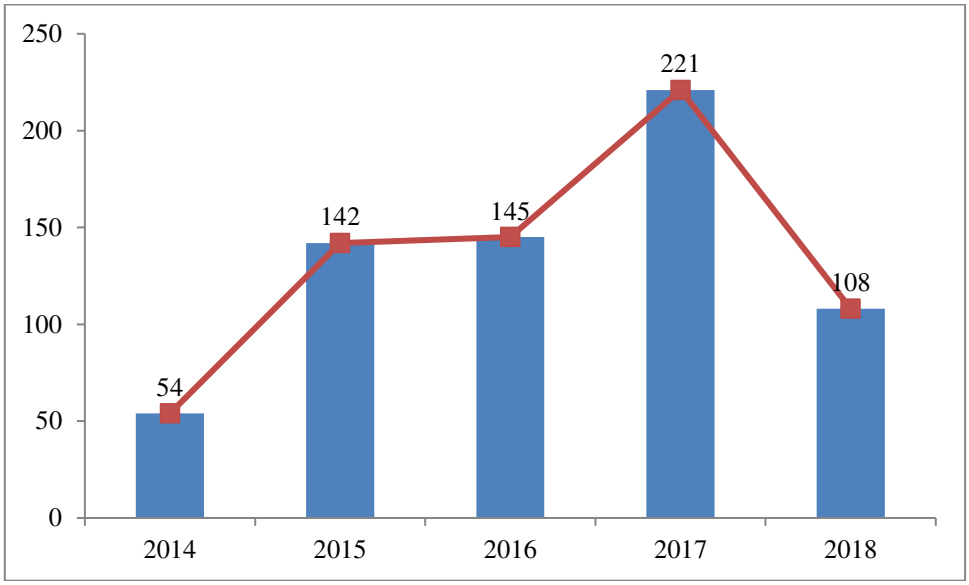


Figura 39. Número de denuncias sobre el Artículo 234 del COIP por años
Fuente: (FGE, 2018)

4.2.10 Capacidad del Ciberdelito

Un aspecto importante a analizar es la capacidad que los responsables de evaluar y juzgar un ciberdelito.

Según la Escuela de Fiscales de la Fiscalía General del Estado, desde el 2017 se han contabilizado un total de 118 capacitados en temas referentes a ciberdelitos.

En la Figura 40 se puede visualizar que las capacitaciones que la Escuela de Fiscales ha realizado, se ha desarrollado en cuatro provincias, en el 2017 en Azuay, Cañar e Imbabura; y en el 2018 en Pichincha.

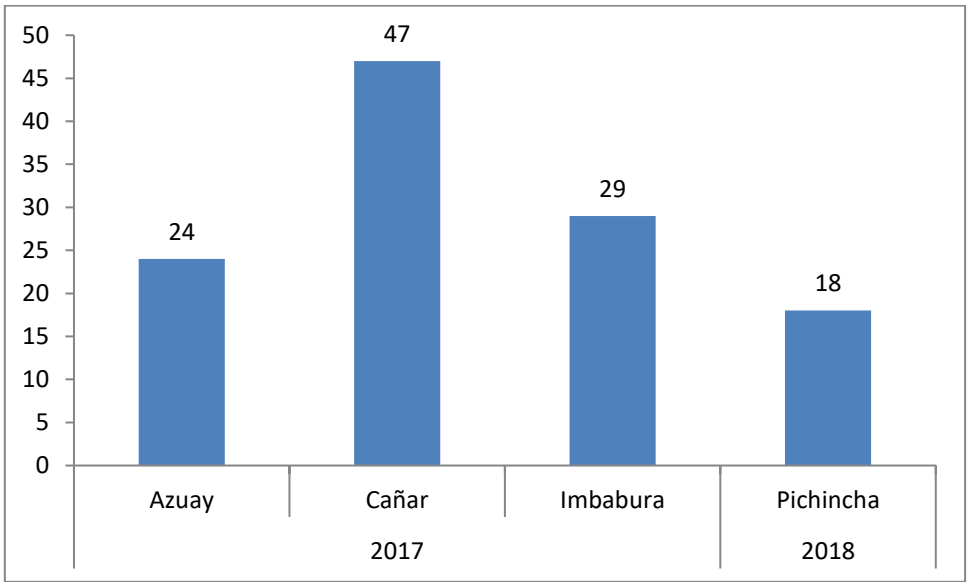


Figura 40. Capacitados en el Ecuador en temas referentes a delitos informáticos
Fuente: (FGE, 2018)

Según (FGE, 2018) Los eventos realizados trataron de varias temáticas de acuerdo a las provincias que se desarrollaron.

Azuay - Introducción al derecho informático (8 horas)

- Época de quiebre
- Consolidación de las NTIC
- Desarticulación en la base de la sociedad
- Desmaterialización del ser humano en un mundo parafísico Homos videns
- La Sociedad de la Información y del Conocimiento
- Vulneración de la intimidad/privacidad
- Recolección y venta de datos
- Software Libre
- Comercio Electrónico
- Características tecnológicas
- Características de E-Commerce
- La Seguridad en el Comercio Electrónico
- Firma Digital/firma electrónico

- Regulación del comercio electrónico
- El contrato electrónico
- Problema iuspositivista internacional del E-Commerce
- Delitos informáticos

(FGE, 2018)

Cañar – Plataformas tecnológicas SICOM – SRT y subsistemas (reportes telefónicos e interceptación de comunicaciones) (16 horas)

- Introducción, antecedentes, y terminología técnica. Marco Constitucional y legal, normativas jurídicas que rigen en los subsistemas, con especial enfoque en la etapa pre-procesal y de juicio.
- Interceptaciones telefónicas
- Reportes telefónicos

(FGE, 2018)

Imbabura – Delitos Informáticos (4 horas)

- Delitos informáticos
- Problemática de ciberseguridad en el Ecuador
- Mitos y verdades sobre la ciberseguridad
- Delitos relacionados con la informático (ciberdelitos, patrimoniales y personales)
- Tratamiento de dispositivos e información dentro de la cadena de custodia.
- El perito cibernético y su función en el proceso penal.

(FGE, 2018)

Pichincha – Causas complejas vinculadas con el cibercrimen: criptomoneda y pornografía infantil (Programa de asistencia contra el crimen transnacional organizado - PAcCTO) (32 horas)

- Generalidades sobre delitos cibernéticos: principales delitos, regulación española, europea e internacional.
- Introducción a las criptomonedas.
- Presentación de un caso o investigación de delitos relacionados con criptomonedas: recomendaciones, buenas prácticas y seguimiento del caso.
- Introducción al rastreo y localización de transacciones fraudulentas realizadas por medios informáticos.
- Buenas prácticas en el rastreo y localización de transacciones fraudulentas realizadas por medios informáticos.
- Herramientas especializadas en la investigación de delitos con criptomonedas y otros delitos cibernéticos relacionados.
- Presentación de un caso o investigación relacionada con transacciones fraudulentas realizadas por medios informáticos.
- Introducción a la pornografía infantil: el tipo penal, la legislación comparada y los retos en la investigación.
- Delitos relacionados con la pornografía infantil.
- En agente encubierto en las redes sociales.
- Comportamiento criminal en relación a la pornografía y explotación infantil.
- Localización y seguimiento de información con contenidos de pornografía infantil.
- El registro de dispositivos de almacenamiento masivo de información y el registro remoto sobre equipos informáticos.
- La pornografía infantil en la Deep Web: Localización y seguimiento de información.

- Métodos para identificar agresiones y agresores a menores dentro de internet y fuentes abiertas.
- Estudios de caso en relación a la explotación infantil: caso práctico

(FGE, 2018)

Esta capacitación estuvo orientada a Fiscales, secretarios y asistentes de los fiscales y servidores de apoyo en el 2017 y lo que va del 2018, tal y como se puede apreciar en la Figura 41.

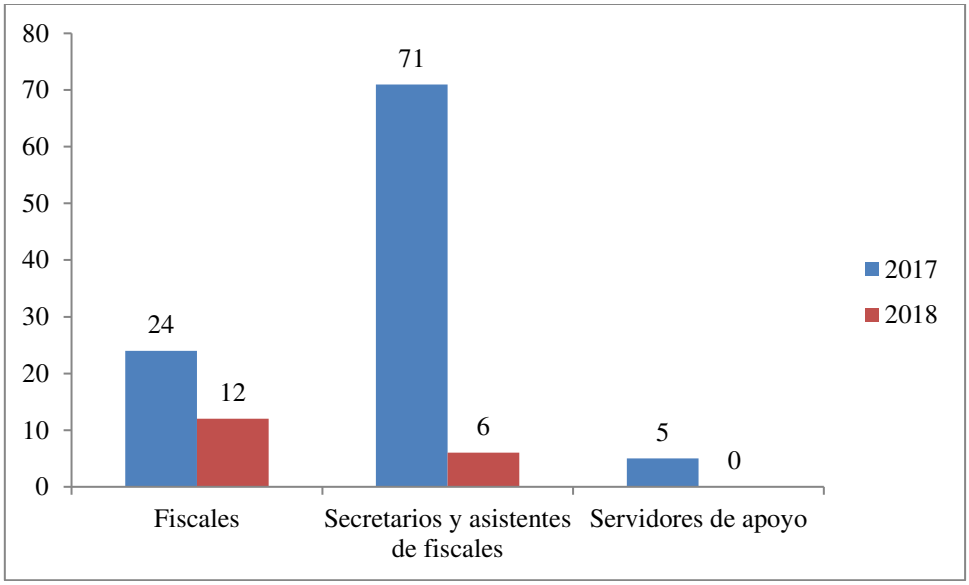


Figura 41. Número de funcionarios capacitados en temas de delitos informáticos.
Fuente: (FGE, 2018)

4.3 Estado de la sensibilización, capacitación y formación

4.3.1 Sensibilización

Como Evidencia O-05 recopilada mediante el instrumento de investigación LBCE-IIC-05 (Ver Anexo C), se muestran la siguiente información facilitada por el Ministerio de Telecomunicaciones y de la Sociedad de la Información.

Desde el MINTEL, a través de los Infocentros Comunitarios, existe una campaña a través de Twitter que empezó desde la primera semana de agosto del 2018, con el Hashtag *#InternetSeguroEc*, en donde se muestra a la ciudadanía memes con información referente a los cuidados que la ciudadanía debe tener ante alguna amenaza que se derive en un delito informático.

Con esta iniciativa se prevé llegar a la ciudadanía sobre los peligros de un uso no correcto del Internet, del cual podrían afectar la integridad de las personas.

A continuación, se puede visualizar algunos memes sobre esta campaña liderada por el MINTEL.

Figura 42. Meme publicitario sobre Grooming
Fuente: (MINTEL, 2018)

Figura 43. Meme publicitario sobre Robo de información
Fuente: (MINTEL, 2018)

Figura 44. Meme publicitario sobre Phising
Fuente: (MINTEL, 2018)

Figura 45. Meme publicitario sobre la prevención de spam
Fuente: (MINTEL, 2018)

Figura 46. Meme publicitario sobre la prevención de scam
Fuente: (MINTEL, 2018)

Figura 47. Meme publicitario sobre el sexting
Fuente: (MINTEL, 2018)

Figura 48. Meme publicitario sobre el vampiring
Fuente: (MINTEL, 2018)

Figura 49. Meme publicitario sobre el ciberacoso o cyberbullying
Fuente: (MINTEL, 2018)

4.3.2 Capacitación

4.3.2.1 MINTEL

Como Evidencia O-05 recopilada mediante el instrumento de investigación LBCE-IIC-05 (Ver Anexo C), se indica que de acuerdo al Plan Nacional de Alistamiento Digital (PLANADI), emitido por el MINTEL en el 2011, es un programa formado por un conjunto de lineamientos y contenidos para la formación de la ciudadanía en TIC. (MINTEL, 2018)

Los cursos que el PLANADI ofrece a la ciudadanía a través de los INFOCENTROS, se muestra en la Figura 50.

Figura 50. Capacitaciones que ofrece el MINTEL a través del PLANADI
Fuente: (MINTEL, 2018)

De las temáticas impartidas en las capacitaciones del MINTEL, los programas sobre TIC para niños y Redes Sociales para jóvenes abarcan temáticas referentes a la Seguridad en el Internet.

Desde el 2017, se han capacitado a 7007 personas en estos dos programas, en la Figura 51 se puede mostrar el número de capacitaciones referentes a TIC para niños y Redes Sociales para jóvenes, seguridad y responsabilidad. (MINTEL, 2018)

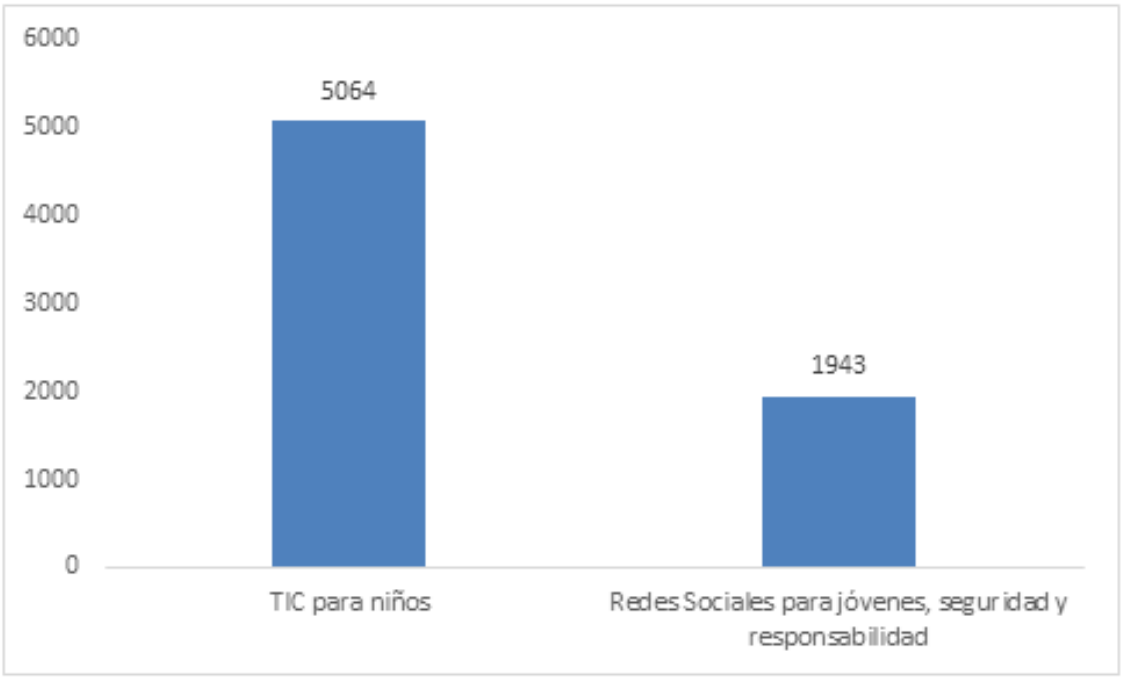


Figura 51. Capacitados en Infocentros sobre Seguridad en Internet
Fuente: (MINTEL, 2018)

En el programa de Redes Sociales para jóvenes, seguridad y responsabilidad ha tenido mucho impacto en la provincia de Azuay en estos dos años, con 281 capacitados, seguido por Chimborazo con 239 y El Oro con 202.

En la

Figura ***52*** se puede mostrar el número de capacitados en todo el Ecuador por provincias donde se encuentran ubicados los Infocentros Comunitarios del MINTEL.

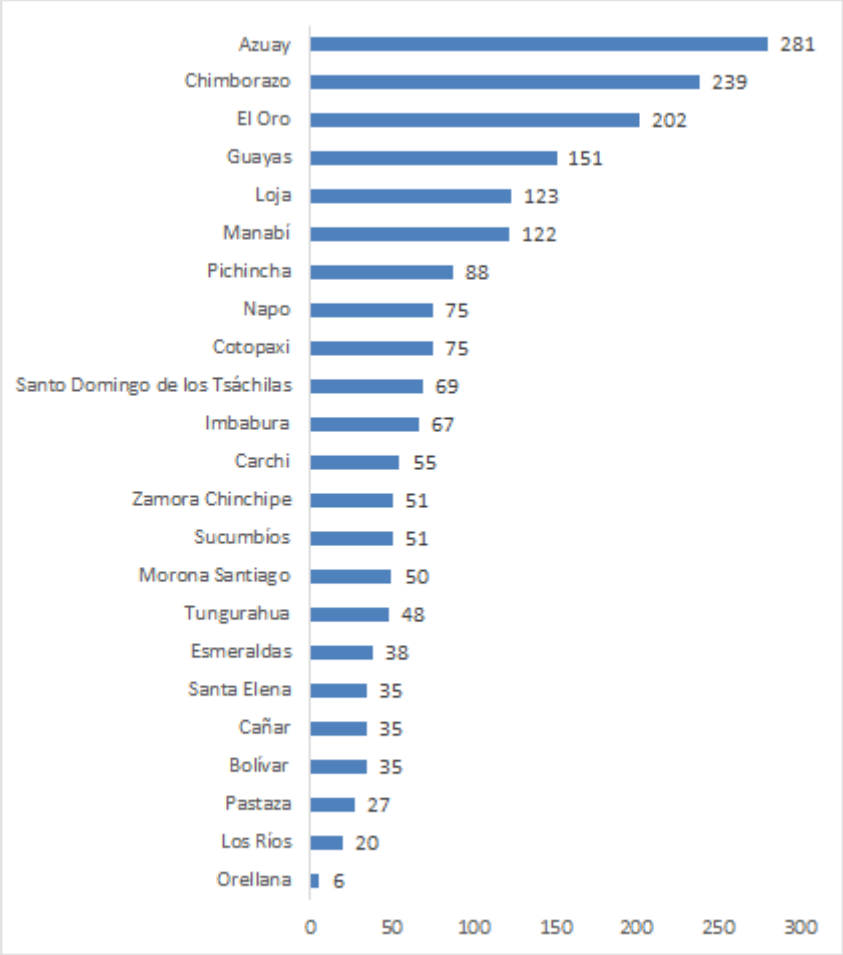


Figura 52. Capacitados en Infocentros sobre Redes Sociales por provincia
Fuente: (MINTEL, 2018)

Dentro del programa TIC para niños, existe una mayor demanda en el Ecuador, con 5064 en el 2017 y 2018, donde se Pichincha tiene el número mayor de capacitados con 521, seguido de Tungurahua con 511 y Loja con 383 capacitados.

En la Figura 53 se puede observar la incidencia de las capacitaciones en el Ecuador mostrado por provincia.

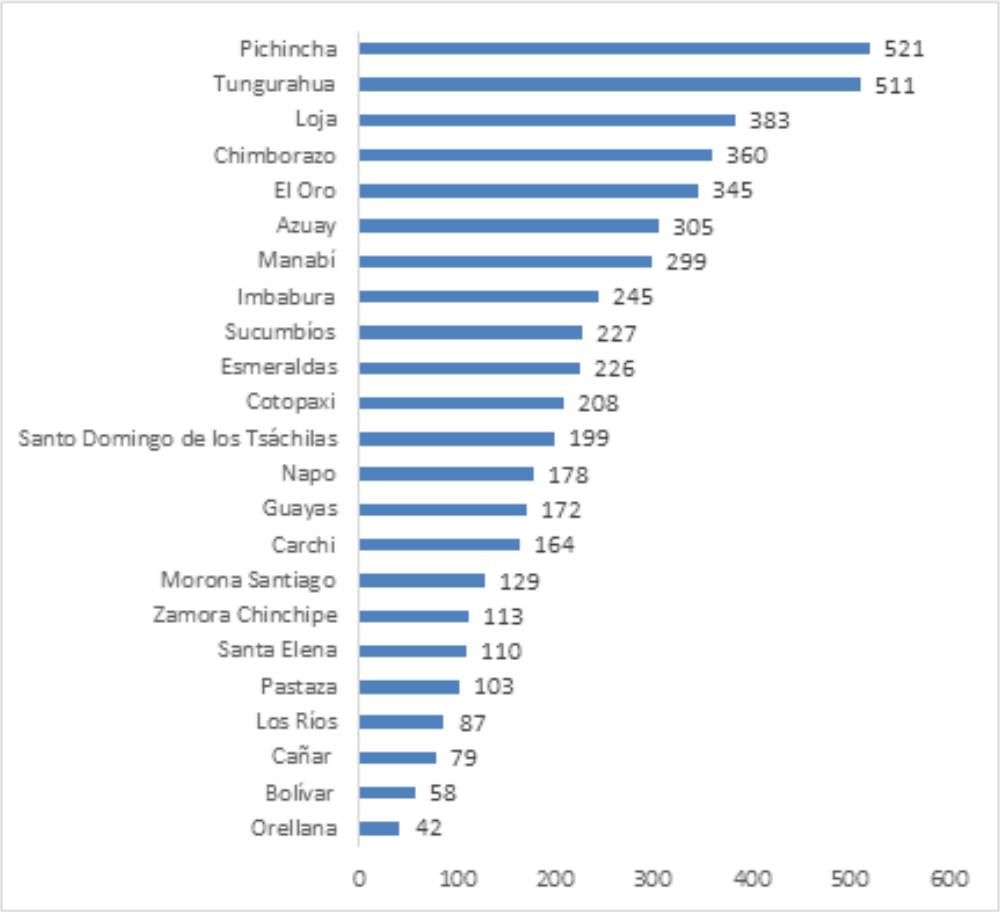


Figura 53. Capacitados en Infocentros sobre TIC por provincia
Fuente: (MINTEL, 2018)

4.3.2.2 EcuCERT

Como Evidencia O-03 recopilada mediante el instrumento de investigación LBCE-IIC-03 (Ver Anexo C), se indica que la ARCOTEL, a través del EcuCERT ha realizado capacitaciones en temas técnicos especializados a instituciones del Estado, cursos para la conformación de nuevos centros de respuesta, además conjuntamente con la Dirección de Comunicación Social de la ARCOTEL se realizan talleres de concientización a instituciones educativas de nivel secundario y superior.

Con referencia a las capacitaciones con temática especializada se pueden mencionar:

- Cursos para la conformación de Centros de Respuesta TRANSITS I, avalada por FIRST, para el Comando de Ciberdefensa del Comando Conjunto de las Fuerzas Armadas del Ecuador y la Escuela Politécnica Nacional.
- Curso de manejo de herramientas de gestión de incidentes informáticos RTIR, al Comando de Ciberdefensa del Conjunto de las Fuerzas Armadas.
- Curso de Informática Forense, para la Unidad de Delitos Informáticos de la Policía Nacional del Ecuador.
- Capacitación en Aseguramiento de Centrales IP-PBX, dictado a personal técnico de los prestadores de servicios de telecomunicaciones y particulares.
- Charlas de concientización sobre delitos informáticos dirigido a universidades e instituciones del Estado.

(ARCOTEL, 2018)

ARCOTEL maneja algunos ejes para la difusión de contenidos referentes a ciberseguridad y destinados a la concientización y prevención de delitos informáticos.

Tabla 9
Temáticas sobre contenidos de ciberseguridad

TEMÁTICA	PÚBLICO OBJETIVO
Charlas de seguridad en redes sociales y ciberbullying	Colegios – Instituciones Educativas
Taller para prevención de ciberdelitos	Universidades e Instituciones del Sector Público

Fuente: (ARCOTEL, 2018)

El número de capacitados donde estos temas se ha podido alcanzar se pueden visualizar en la Figura 54.

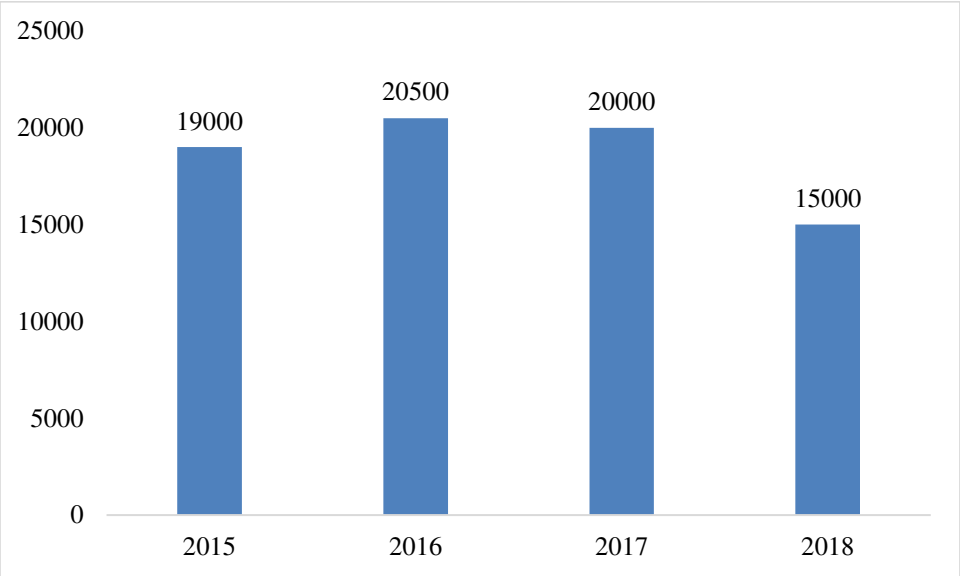


Figura 54. Número de capacitados aproximados por el EcuCERT
Fuente: (ARCOTEL, 2018)

En lo que va del 2018, son aproximadamente 15000 personas, que han recibido charlas y talleres de concientización en los distintos ejes. (ARCOTEL, 2018).

4.3.3 Formación

4.3.3.1 Formación Académica

Como Evidencia O-06 recopilada mediante el instrumento de investigación LBCE-IIC-06 (Ver Anexo C), se muestran la siguiente información facilitada por la Secretaría de Educación Superior, Ciencia y Tecnología.

Actualmente, en el Ecuador no existen ofertas académicas de cuarto nivel específicas de Seguridad de la Información o Ciberseguridad, pero existen otras maestrías, especializaciones o doctorados que están relacionados a los Sistemas Informáticos o la Gestión de la Información, donde se incorporan en sus mallas curriculares, asignaturas sobre seguridad de la información que son ofertadas por las instituciones de educación superior.

En la Figura 55 se puede apreciar el número de ofertas académicas de cuarto nivel en las Universidades y Escuelas Politécnicas del Ecuador en la cual se adjunta dentro de su malla curricular, asignaturas referentes a seguridad de la información y/o ciberseguridad.

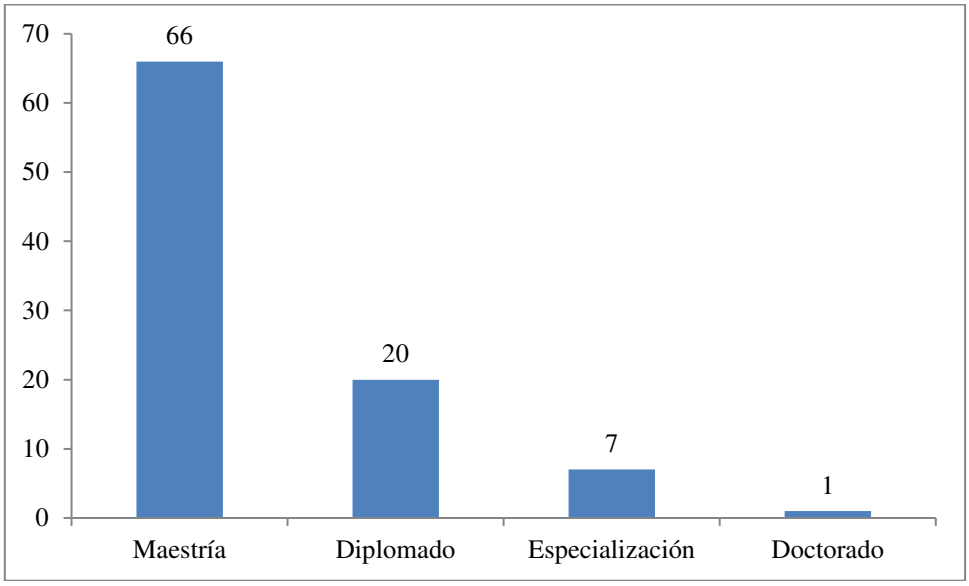


Figura 55. Ofertas académicas de cuarto nivel en Universidades ecuatorianas
Fuente: (SENESCYT, 2018)

Según (SENESCYT, 2018), dentro de las ofertas académicas 2009 y 2013, la Escuela Politécnica Nacional es la única institución que ofrece un Doctorado en el Ecuador en una especialización que dentro de su pensum incluiría la formación de Seguridad de la Información y/o Ciberseguridad, denominado "Doctorado en Informática". En la Tabla 10 se puede visualizar el número de maestrías, diplomados, especializaciones o doctorados que las Universidades y Escuelas Politécnicas del país ofrecen de acuerdo a las ofertas académicas 2009 y 2013.

Tabla 10
Ofertas de postgrado donde imparten Seguridad de la Información y/o Ciberseguridad

UNIVERSIDADES Y ESCUELAS POLITÉCNICAS	MAESTRIA	DIPLOMADO	ESPECIALIZACION	DOCTORADO
Escuela Politécnica Nacional	2	1	1	1
Escuela Superior Politécnica Agropecuaria de Manabí	1	0	0	0

CONTINÚA

UNIVERSIDADES Y ESCUELAS POLITÉCNICAS	MAESTRIA	DIPLOMADO	ESPECIALIZACION	DOCTORADO
Escuela Superior Politécnica de Chimborazo	4	1	0	0
Escuela Superior Politécnica del Litoral	7	5	0	0
Pontificia Universidad Católica del Ecuador	6	3	1	0
Universidad Andina Simón Bolívar	2	0	3	0
Universidad Católica De Cuenca	3	0	0	0
Universidad Central Del Ecuador	4	1	0	0
Universidad De Cuenca	2	1	0	0
Universidad De Guayaquil	1	0	0	0
Universidad De Las Américas	2	0	0	0
Universidad De Las Fuerzas Armadas (ESPE)	8	0	0	0
Universidad Estatal de Milagro	1	0	0	0
Universidad Laica Eloy Alfaro de Manabí	2	2	1	0
Universidad Nacional de Loja	0	1	0	0
Universidad Particular de Especialidades Espíritu Santo	4	0	0	0
Universidad Particular Internacional SEK	1	0	0	0
Universidad Regional Autónoma de Los Andes	5	2	1	0
Universidad Técnica de Ambato	5	1	0	0
Universidad Técnica de Cotopaxi	1	0	0	0
Universidad Tecnológica ECOTEC	1	0	0	0
Universidad Tecnológica Empresarial de Guayaquil	1	0	0	0
Universidad Tecnológica Israel	1	1	0	0
Universidad UTE	2	1	0	0

Fuente: (SENESCYT, 2018)

En la Tabla 11, se puede apreciar el número de matriculados en las carreras de cuarto nivel ofertadas por las Instituciones de Educación Superior desde el 2015 al 2019.

Tabla 11

Matriculados en carreras de cuarto nivel afines a Ciberseguridad

INSTITUTO	NOMBRE CARRERA	TOTAL MATRICULADOS
Escuela Politécnica Nacional	Maestría en ciencias de la computación e informática	6
Escuela Politécnica Nacional	Maestría en gestión de las comunicaciones y tecnologías de la información	353
Escuela Superior Politécnica Agropecuaria de Manabí	Tecnologías de la información	50
Escuela Superior Politécnica del Litoral	Maestría en seguridad informática	16
Escuela Superior Politécnica del Litoral	Maestría en sistemas de información gerencial	242
Universidad Andina Simón Bolívar	Educación y nuevas tecnologías de la información y la comunicación	27
Universidad Andina Simón Bolívar	Especialización superior en educación y nuevas tecnologías de la información y la comunicación	80
Universidad Católica de Cuenca	Tecnologías de la información	145
Universidad de Cuenca	Maestría en gestión estratégica de tecnologías de la información	74
Universidad de las Américas	Gerencia de sistemas y tecnología empresarial	173
Universidad de las Américas	Maestría en gerencia de sistemas y tecnologías de la información	802
Universidad De las Fuerzas Armadas (ESPE)	Maestría en gerencia de sistemas	60
Universidad De las Fuerzas Armadas (ESPE)	Maestría en gestión de sistemas de información e inteligencia de negocios	162
Universidad Particular de Especialidades Espíritu Santo	Maestría en auditoria de tecnologías de la información	108
Universidad Particular Internacional SEK	Tecnologías de la información	689
Universidad Tecnológica Empresarial de Guayaquil	Sistemas de información gerencial	72
Universidad UTE	Sistemas de información	24

Fuente: (SENESCYT, 2018)

De acuerdo a los becarios ecuatorianos, que han tenido formación referente a ciberseguridad o seguridad de la información, han existido un total de 52 becarios desde el 2008 hasta el 2017.

Los países de mayor demanda de estudios en este campo son Reino Unido, Argentina, Chile y Estados Unidos, tal y como se muestra en la Tabla 12.

Tabla 12

Países con mayor número de estudiantes de postgrado sobre seguridad de la información

País de Estudios	Total
Total	**52**
Reino Unido	22
Argentina	7
Chile	7
Estados Unidos	5
España	4
Australia	3
Noruega	1
Francia	1
Suecia	1
Italia	1

Fuente: (SENESCYT, 2018)

Existen estudiantes que se encuentran en diferentes etapas de su formación como adjudicatarios, en compensación, en estudios o ex adjudicatarios en las distintas universidades del mundo, tal y como se muestra en la Tabla 13.

Tabla 13

Oferta de estudios de postgrado de universidades del mundo y becarios ecuatorianos

Universidad de Estudios	País de Estudios	Nivel de Estudios	Carrera	2008	2011	2012	2013	2014	2015	2017	Total
Universidad de Buenos Aires	Argentina	Maestría	Seguridad informática	0	1	2	1	1	1	0	**6**
Universidad de Buenos Aires	Argentina	Maestría	Seguridad informática	0	0	0	1	0	0	0	**1**
Universidad de Griffith	Australia	Maestría	Tecnología de la información importante en redes y seguridad	0	0	1	0	0	0	0	**1**
Universidad de Monash	Australia	Maestría	Redes y seguridad	0	0	0	0	1	0	0	**1**
Universidad de Deakin	Australia	Maestría	Redes y seguridad	0	0	1	0	0	0	0	**1**
Universidad de Santiago de Chile	Chile	Maestría	Seguridad peritaje y auditoria en procesos informáticos	0	0	1	2	4	0	0	**7**
Universidad Rovira I Virgili	España	Maestría	Seguridad informática y sistemas inteligentes	0	1	0	0	0	0	0	**1**
Universidad Politécnica de Madrid	España	Maestría	Ciberseguridad	0	0	0	0	0	0	1	**1**
Universidad Internacional de La Rioja	España	Maestría	Seguridad informática	0	0	0	0	0	0	2	**2**
Instituto Tecnológico de Illinois	Estados Unidos	Maestría	Cyber forense y seguridad	0	0	1	0	0	0	0	**1**
Universidad de Stony Brook	Estados Unidos	Maestría	Seguridad y privacidad	0	0	1	0	0	0	0	**1**
Universidad Northeastern	Estados Unidos	Maestría	Software y seguridad sistemas	0	0	0	1	0	0	0	**1**

CONTINÚA

Universidad de Estudios	País de Estudios	Nivel de Estudios	Carrera	2008	2011	2012	2013	2014	2015	2017	Total
Instituto de Tecnología de Georgia	Estados Unidos	Maestría	Seguridad informática	0	0	0	0	0	0	1	**1**
Universidad De Nueva York	Estados Unidos	Maestría	Ciberseguridad	0	0	0	0	1	0	0	**1**
Universidad Toulouse Ii Le Mirail	Francia	Doctorado	Seguridad informática	1	0	0	0	0	0	0	**1**
Universidad de Calabria	Italia	Doctorado	Software y seguridad de sistemas	0	0	1	0	0	0	0	**1**
Universidad Noruega de Ciencia y Tecnología	Noruega	Maestría	Redes de comunicación y servicios con especialización en seguridad de la información	0	0	0	0	1	0	0	**1**
Universidad de Greenwich	Reino Unido	Maestría	Informática forense y ciberseguridad	0	0	0	2	0	0	0	**2**
Universidad de Southampton	Reino Unido	Maestría	Seguridad cibernética	0	0	0	0	2	0	0	**2**
Universidad de Southampton	Reino Unido	Maestría	Seguridad cibernética	0	0	0	0	2	0	0	**2**
Colegio Universitario de Londres	Reino Unido	Maestría	Seguridad informática	0	0	0	0	0	0	1	**1**
Colegio Universitario de Londres	Reino Unido	Maestría	Seguridad informática	0	0	0	0	1	0	0	**1**
Universidad Abertay	Reino Unido	Maestría	Programa de la ciencia en la ética piratería informática y seguridad	0	0	1	0	0	0	0	**1**
Universidad de Birmingham	Reino Unido	Maestría	Ciencias en seguridad computacional	0	0	0	1	0	0	0	**1**
Universidad de	Reino	Maestría	Seguridad computacional	0	0	0	1	0	0	0	**1**

CONTINÚA

Universidad de Estudios	País de Estudios	Nivel de Estudios	Carrera	2008	2011	2012	2013	2014	2015	2017	Total
Birmingham	Unido										
Universidad de Birmingham	Reino Unido	Maestría	Seguridad informática	0	0	0	0	1	0	0	**1**
Universidad de Edimburgo	Reino Unido	Maestría	Seguridad avanzada y analisis forense digital	0	0	1	0	0	0	0	**1**
Universidad de Greenwich	Reino Unido	Maestría	Ciencias en seguridad de la informacin y auditoria	0	0	1	0	0	0	0	**1**
Universidad de Oxford	Reino Unido	Maestría	Software y sistemas de seguridad	0	0	0	0	1	0	0	**1**
Universidad de Sheffield	Reino Unido	Maestría	Sistemas de seguridad de la información	0	0	1	0	0	0	0	**1**
Universidad de Southampton	Reino Unido	Maestría	Seguridad computacional	0	0	0	0	1	0	0	**1**
Universidad de York	Reino Unido	Maestría	Ciberseguridad	0	0	0	1	0	0	0	**1**
Universidad Edinburgh Napier	Reino Unido	Maestría	Seguridad avanzada y analisis forense digital	0	0	0	1	0	0	0	**1**
Colegio Universitario de Londres	Reino Unido	Doctorado	Ciencias de la seguridad	0	0	0	0	1	0	0	**1**
Universidad De Southampton	Reino Unido	Maestría	Seguridad cibernética	0	0	0	0	0	0	1	**1**
Universidad De Manchester	Reino Unido	Maestría	Seguridad informática	0	0	1	0	0	0	0	**1**
Universidad De Estocolmo	Suecia	Maestría	Seguridad de la información	0	0	0	0	0	0	1	**1**
		Total		1	2	13	11	17	1	7	**52**

Fuente: (SENESCYT, 2018)

4.3.3.2 Pacto Operativo del Gobierno Nacional con la niñez y adolescencia por un Internet Seguro

Como Evidencia O-07 recopilada mediante el instrumento de investigación LBCE-IIC-07 (Ver Anexo C), se muestran la siguiente información facilitada por el Ministerio de Educación.

El 1 de junio del 2018, en la Asamblea Nacional del Ecuador, se firmó el "Pacto Operativo del Gobierno Nacional con la niñez y adolescencia por un Internet Seguro"suscrito por el Ministerio de Inclusión Social (MIES, el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) y el Ministerio de Educación y Deporte (MINEDUC) donde se fijan compromisos para brindar condiciones responsables para el uso del Internet como una herramienta segura en el desarrollo de los niños, niñas y adolescentes. (MIES, 2018)

Entre los compromisos se detallan:

- Formular un plan de acción que incluyan estrategias de capacitación, prevención y protección contra la violencia en internet enfocado a niños, niñas y adolescentes.
- Desarrollar y ejecutar campañas de integrales de educación y comunicación sobre sus derechos y garantías, así como el uso adecuado del Internet, formulando una adecuada prevención, reducir riesgos, peligros y amenazas que atentan contra la niñez y adolescencia ecuatoriana.
- Coordinar campañas y procesos de difusión y capacitación a través de la red de infocentros en el Ecuador.

(MIES; MINTEL; MINEDUC, 2018)

4.4 Estado de la cooperación internacional

4.4.1 Afiliaciones internacionales

Como Evidencia O-03 recopilada mediante el instrumento de investigación LBCE-IIC-03 (Ver Anexo C), se muestran la siguiente información facilitada por la Agencia de Regulación y Control de las Telecomunicaciones.

El EcuCERT es parte de la red de confianza FIRST (Forum of Incident Response and Security Teams) desde el 2 de octubre de 2014, FIRST es la principal organización y líder mundial reconocido en respuesta a incidentes. La membresía del EcuCERT es de tipo "Full Member". Actualmente FIRST cuenta con 438 miembros en 90 países distribuidos en África, América, Asia, Europa y Oceanía.

Además, el EcuCERT pertenece a organizaciones y redes de confianza como:

- LACNIC (Registro de Direcciones de Internet de América Latina y Caribe) [4]
- UIT (Unión Internacional de Telecomunicaciones)
- OEA (Organización de Estados Americanos)
- En proceso CERT/CC de Carnegie Mellon

Estas asociaciones permiten trabajar proactivamente la gestión de incidentes de seguridad que puedan afectar a las redes y/o servicios de telecomunicaciones en el Ecuador.

[4] Es una organización no gubernamental internacional donde su principal función es la asignación y administración de los recursos de numeración de Internet (IPv4, IPv6), Números Autónomos y Resolución Inversa para la región.

El EcuCERT, trabaja con “Feeds” a nivel mundial como es el caso de ShadowServer, Kaspersky, Team Cymru, entre otros, que permiten descubrir de manera inmediata las vulnerabilidades que existen en la red de internet.

4.4.2 Convenio de Budapest

Como Evidencia O-08 recopilada mediante el instrumento de investigación LBCE-IIC-08 (Ver Anexo C), se muestran la siguiente información facilitada por el Ministerio de Telecomunicaciones y de la Sociedad de la Información.

El convenio sobre la ciberdelincuencia es el primer tratado internacional suscrito el 23 de noviembre del 2001 donde su objetivo es hacer frente a los ciberdelitos mediante la coordinación y armonización de las leyes nacionales la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones.

Los delitos que se tratan en el Convenio de Budapest principalmente son las infracciones de derechos de autor, fraude informático, la pornografía infantil, los delitos de odio y violaciones de seguridad de red. (Council Of Europe, 2001)

Dicho convenio consta de tres ejes esenciales.

Eje 1. Delitos informáticos donde se establece un catálogo de figuras dedicadas a penar las modalidades de criminalidad informática.

Eje 2. Normas procesales donde se establecen los procedimientos para salvaguardar la evidencia digital, así como también las herramientas relacionadas con la manipulación de esta evidencia.

Eje 3. Normas de cooperación internacional en el cual se establecen las reglas de cooperación para investigar cualquier delito que involucre evidencia digital, ya sean delitos tradicionales o informáticos. (Pastorino, 2017)

Los países firmantes al Convenio pertenecientes a la región de América son:

- Argentina
- Canadá
- Chile
- Colombia
- Costa Rica
- Estados Unidos
- República Dominicana
- México
- Panamá

Al momento, Ecuador no pertenece al grupo de los países firmantes al Convenio de Budapest, el cual nos impide desarrollar investigación sobre delitos informáticos ya que no se cuenta con estas herramientas y procedimientos para la prevención y corrección de os delitos, vulnerabilidades y amenazas informáticas.

4.5 Estado de la institucionalidad

4.5.1 Entidades responsables

Como Evidencia O-08 recopilada mediante el instrumento de investigación LBCE-IIC-08 (Ver Anexo C), se muestran la siguiente información facilitada por el Ministerio de Telecomunicaciones y de la Sociedad de la Información.

a) Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL)

De acuerdo a la (Asamblea Nacional, 2015) en su Artículo 140, el MINTEL "*...es el órgano rector de las Telecomunicaciones y de la Sociedad de la Información, informática tecnologías de la información y las comunicaciones y de la seguridad de la información. A dicho órgano le corresponde el establecimiento de políticas, directrices y planes aplicables en tales áreas para el desarrollo de la sociedad de la información*".

b) Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL)

La ARCOTEL, a través del EcuCERT creado mediante Resolución ST-2014-0247 del 18 de julio de 2014 por la Ex - Superintendencia de Telecomunicaciones se encarga de "*contribuir a la seguridad de las redes de telecomunicaciones de todo el país y así como el uso de la red de Internet*".

La "Comunidad Objetivo" del EcuCERT de la ARCOTEL, está definido como las organizaciones a las que el centro brinda sus servicios de manera inmediata y se han clasificado de la siguiente manera:

- Los prestadores de servicios de telecomunicaciones, legalmente reconocidos para brindar servicios de acceso a telecomunicaciones a través de redes. (ISP).
- Las instituciones del sector de gobierno que conforman el Estado Ecuatoriano.
- Las empresas privadas y la ciudadanía en general, de acuerdo a la solicitud del requerimiento.

(ARCOTEL, 2018)

c) Comando de Ciberdefensa (COCIBER)

El COCIBER fue creado mediante Acuerdo Ministerial Nro. 281 del 12 de septiembre del 2014 por el Ministerio de Defensa Nacional con el fin de "defender, explotar el dominio cibernético y responder ante incidentes o amenazas que atenten la infraestructura crítica estratégica digital de las Fuerzas Armadas y del Estado; a través de la conducción de operaciones de ciberdefensa, a fin de contribuir a la misión del Comando Conjunto".

d) Fiscalía General del Estado (FGE)

Es la institución que garantiza el acceso a la justicia y el respeto de los Derechos Humanos, con Talento Humano comprometido con el servicio a la ciudadanía. Para ello debe dirigir la investigación pre-procesal y procesal penal basada en el Código Orgánico Integral Penal (COIP). (FGE, 2018).

4.5.2 Funciones del EcuCERT

Como Evidencia O-03 recopilada mediante el instrumento de investigación LBCE-IIC-03 (Ver Anexo C), se muestran la siguiente información facilitada por la Agencia de Regulación y Control de las Telecomunicaciones.

El EcuCERT es reconocido como un CIRT (Critical Incident Response Team) nacional oficial de acuerdo al Índice mundial de ciberseguridad y perfiles de ciberbienestar. (UIT, 2015), por tal motivo es necesario determinar las acciones que esta institución realiza para gestionar la ciberseguridad en el país.

Los servicios que brinda el EcuCERT a la comunidad y a la ciudadanía responden a dos modalidades de carácter *"proactivo*" y *"reactivo"*, con el objetivo de prevenir y responder ante eventos que propicien la ejecución de una explotación de una vulnerabilidad de las redes, y que ésta se pueda convertir en un incidente de seguridad de la información en tiempo real,

que pudiese afectar las infraestructuras críticas de las redes de telecomunicaciones a nivel nacional.

Los servicios proactivos, definidos por el EcuCERT son:

- Servicios de detección de intrusos.
- Difusión de información relacionada con la seguridad de la información.

Los servicios reactivos son:

- Análisis y alertas tempranas de vulnerabilidades de seguridad de la información.
- Análisis de incidentes de seguridad informática.
- Respuesta de incidentes informáticos en el sitio.
- Coordinación nacional e internacional en la gestión de incidentes de seguridad de la información.

Además de estos, el EcuCERT de la ARCOTEL provee los siguientes servicios:

- Observatorio de tecnología.
- Capacitación integral en seguridad de la información.
- El EcuCERT posee una infraestructura propia, lo que significa que cuenta con enlaces dedicados, servidores propios para la gestión de página web, correo, almacenamiento, red interna propia. Además cuenta con un servidor especializado en tratamiento forense de la información (FRED), y un laboratorio de redes en las que se realizan todas las pruebas de malware dentro de un ambiente controlado.

La función principal es de coordinar y gestionar vulnerabilidades e incidentes informáticos reportados desde los steakholders, realizando un registro de los casos de manera ordenada y cronológica en la plataforma diseñada para la realización de esta actividad.

A través de la ARCOTEL se ha generado la normativa relacionada con la gestión de incidentes y vulnerabilidades, con el fin de que los prestadores de servicios del régimen general de telecomunicaciones ofrezcan las condiciones mínimas necesarias para asegurar la información de sus infraestructuras y de la de sus usuarios finales.

4.6 Informe Ejecutivo para la proyección de una Política Nacional

El presente informe ejecutivo se muestra con mayor detalle en el Anexo B.

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- A través del método Tankyu, desarrollado desarrollada por el Instituto de Computación de Kobe y el desarrollo del árbol de problemas mediante el método PCM (*Project Cycle Management*), se determinan los problemas que el Ecuador tiene referente a la gestión de la Ciberseguridad, por lo que puede destacar la problemática principal es la carencia de una Política/Estrategia Nacional de Ciberseguridad, que permita dar directrices o líneas de acción de manera integral a todos los sectores para fortalecer la gestión del riesgo del ciberespacio.
- A través de la selección de factores, se determinaron los aspectos de interés de la ciberseguridad para realizar la investigación de campo, y con ello determinar los actores fundamentales en levantar la línea base de la Ciberseguridad en el país. Así es como se establece los siguientes factores: Infraestructura de la información, marco penal, sensibilización, capacitación y formación, cooperación nacional e internacional e institucionalidad.
- La institución encargada de efectuar operaciones de ciberdefensa para proteger y defender la infraestructura crítica e información estratégica del Estado es el Comando de Ciberdefensa (COCIBER), pero en la actualidad dicha entidad no evidencia información que permita establecer un modelo de gestión organizacional, personal, formación, capacitación, etc; así mismo de una metodología que permita definir, clasificar e identificar las infraestructuras críticas en el país.
- El Ministerio de Telecomunicaciones y de la Sociedad de la Información ha evaluado a agosto de 2018 a 64 instituciones de la Administración Pública en el marco del Esquema Gubernamental de la Seguridad de la Información, donde solo el 15.63% tiene una

calificación de “buena”, y un 71.88% tiene una calificación de regular. Estas evaluaciones están basadas en dos fases basadas en las recomendaciones de la NTE INEN ISO 27002, y no contemplan evaluaciones de Planes de contingencia, planes de resiliencia o gestión de la continuidad del negocio.

- El Código Orgánico Integral Penal, aprobado en el 2014 estipula delitos informáticos basados en pornografía infantil, interceptación ilegal de datos, accesos no consentidos a sistemas informáticos, telemáticos, ataques a la integridad de los sistemas informáticos, entre otros. La mayoría de penas de dichos delitos se establecen de 3 a 5 años de privación de libertad.
- La Fiscalía General del Estado, a través de la Escuela de Fiscales realiza capacitación a sus funcionarios. En el 2017 y 2018 se ha capacitado un total de 118 funcionarios, de los que se encuentran fiscales, secretarios y asistentes de fiscales y servidores de apoyo.
- El Ministerio de Telecomunicaciones y de la Sociedad de la Información ha llevado campañas de concienciación sobre peligros del Internet a través de Twitter denominada “Internet SeguroEc” en el cual se quiere llegar a la ciudadanía con afiches y memes con información sobre dichas amenazas y como prevenirlas.
- La Agencia de Regulación y Control de las Telecomunicaciones ha llevado campañas sobre charlas de seguridad en redes sociales y cyberbulling, y talleres de prevención de ciberdelitos alrededor de 15000 beneficiarios de instituciones educativas, universidades e instituciones del sector público.
- Con el fin de brindar condiciones responsables para el uso del Internet como una herramienta segura en el desarrollo de los niños, niñas y adolescentes, se suscribió en el 2018 el “Pacto Operativo del Gobierno Nacional con la niñez y adolescencia por un Internet Seguro”, en donde de manera coordinada, el MINTEL, MINEDUC y el MIES se comprometen en establecer estrategias de capacitación, prevención y protección contra la

violencia en internet enfocado a niños, niñas y adolescentes, establecer campañas sobre educación y comunicación sobre derechos y garantías así como el uso responsable de Internet.

- En cooperación internacional, la ARCOTEL ha logrado suscribirse a la red de confianza FIRST, con el fin de contar con la retroalimentación de sus miembros sobre respuesta a incidentes; además se gestiona con otras entidades de Gobierno la posibilidad de formar parte del Convenio de Budapest o convenio sobre la ciberdelincuencia.
- Es necesario el desarrollo de una Política y/o Estrategia Nacional de Ciberseguridad que dicte lineamientos y acciones precisas aplicados a los campos técnicos, legales y políticos con el fin de fomentar un uso responsable del ciberespacio, además de promover el trabajo conjunto de todos los sectores, en base a la línea base presentada en la presente investigación.

5.2 Recomendaciones

- Establecer la información presentada en la línea base como insumo para formular conjuntamente con los actores involucrados en la Cibseseguridad y ciberdefensa del país, las acciones que la Política/Estrategia Nacional de Ciberseguridad deberá tener en beneficio de la nación.
- Que el Comando de Ciberdefensa del Comando Conjunto de las Fuerzas Armadas plantee una metodología para la definición y clasificación de las infraestructuras críticas del Ecuador, su tratamiento y gestión en caso de un posible incidente cibernético.
- Gestionar con el Ministerio de Relaciones Exteriores y Movilidad Humana, en conjunto con las entidades de Gobierno involucradas en la Ciberseguridad y Ciberdefensa, la adhesión del Ecuador al grupo de los países que conforman el Convenio de Budapest.

- Gestionar con el Ministerio de Educación, la inclusión de asignaturas referentes a la Ciberseguridad en las mallas curriculares de Educación básica y media, con el fin de fomentar la cultura de la ciberseguridad en los estudiantes.
- Fomentar la creación de carreras de pregrado y posgrado referentes a Seguridad de la Información y/o Ciberseguridad, y así impulsar el mercado laboral y la investigación en el tema.
- Tomar acercamientos con la Organización de Estados Americanos (OEA), en el desarrollo de la Política/Estrategia Nacional de Ciberseguridad, así como en el fortalecimiento de las capacidades de la ciberseguridad en los funcionarios públicos a través de talleres, conferencias, capacitaciones, etc, debido a la experiencia que dicho organismo internacional ha llevado a través de la Comisión Interamericana en contra del Terrorismo (CICTE) en formular las acciones para fortalecer la ciberseguridad en la región.

BIBLIOGRAFÍA

Acurio, S. (2017). ITAhora. *Panorama legal sobre ciberseguridad en el Ecuador*. Quito, Pichincha, Ecuador. Obtenido de http://www.itahora.com/actualidad/seguridad/panorama-legal-sobre-ciberseguridad-en-ecuador/

Aguirre Ponce, A. A. (2017). Ciberseguridad en Infraestructuras Críticas de Información. Buenos Aires, Argentina.

ARCOTEL. (2018). EcuCERT - Vulnerabilidades e incidentes en el Ecuador. Quito, Ecuador.

Asamblea Nacional. (2014). Código Orgánico Integral Penal. Ecuador.

Asamblea Nacional. (18 de febrero de 2015). Ley Orgánica de Telecomunicaciones. Ecuador. Obtenido de https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2016/05/Ley-Org%C3%A1nica-de-Telecomunicaciones.pdf

CARI. (noviembre de 2013). *Ciberdefensa - Ciberseguridad - Riesgos y amenazas.* Obtenido de http://www.cari.org.ar/pdf/ciberdefensa_riesgos_amenazas.pdf

CEDIA. (2017). Estado de las Tecnologías de la Información y Comunicación en las Universidades del Ecuador. Cuenca, Ecuador.

COCIBER. (2018). Infraestructuras críticas Ecuador.

Council Of Europe. (23 de noviembre de 2001). Serie de tratados Nro. 185. *Convenio sobre la ciberdelincuencia*. Budapest, Hungria.

Deloitte. (2017). *Seguridad de la Información en Ecuador*. Obtenido de https://www2.deloitte.com/content/dam/Deloitte/ec/Documents/deloitte-analytics/Estudios/SeguridadInformacion2017.pdf

Diario ABC Tecnología. (2016). *Ciberseguridad: tendencias que marcarán el 2016*. Obtenido de http://www.abc.es/tecnologia/redes/abci-ciberseguridad-tendencias-marcara-2016-201512280112_noticia.html

El Financiero. (2017). *4 de cada 5 países en AL no tienen estrategias de ciberseguridad.* Obtenido de http://www.elfinanciero.com.mx/tech/de-cada-paises-en-al-no-tienen-estrategias-de-ciberseguridad

ESET. (2017). *Ataques a infraestructuras críticas, ¿modalidad inminente en 2017?* Obtenido de Welivesecuriry: https://www.welivesecurity.com/la-es/2017/01/04/ataques-a-infraestructuras-criticas-2017/

FGE. (2015). *Los delitos informáicos van desde el fraude hasta el espionaje.* Obtenido de https://www.fiscalia.gob.ec/los-delitos-informaticos-van-desde-el-fraude-hasta-el-espionaje/

FGE. (11 de junio de 2018). Denuncias sobre delitos informáticos. Quito, Ecuador.

FGE. (2018). Información de eventos de capacitación relacionados a la investigación de delitos informáticos. Quito, Pichincha, Ecuador.

FGE. (2018). Planificación Estratégica. Obtenido de ¿Qué es la Fiscalía?: https://www.fiscalia.gob.ec/institucion/

González, C. (4 de abril de 2018). *Emagister.* Obtenido de La importancia de la ciberseguridad en el mundo empresarial: https://www.emagister.com/blog/la-importancia-la-ciberseguridad-mundo-empresarial/

Guerrero, F. (2018). *La Ciberseguridad Industrial en Ecuador*. Obtenido de Centro de Ciberseguridad Industrial CCI: https://www.cci-es.org/web/cci/detalle-pais/-/journal_content/56/10694/445446;jsessionid=6F289DACA35AAC232BF9011B25E47850

Hernández, J. C. (27 de febrero de 2018). *Estrategias nacionales de Ciberseguridad en América Latina*. Obtenido de Grupo de Estudios en Seguridad Internacional - GESI: http://www.seguridadinternacional.es/?q=es/content/estrategias-nacionales-de-ciberseguridad-en-am%C3%A9rica-latina

ISACA. (19 de Junio de 2014). 8° B: Secure Conference. Monterrey, México.

ISO. (2005). ISO/IEC 17799. *Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información*.

ISO. (2010). ISO/IEC 27032. *Information technology — Security techniques — Guidelines for Cybersecurity*.

JICA - KIC. (julio de 2017). JICA Workshop. *Problem and objetive analysis based on PCM Method*. Kobe, Kansai, Japón.

Kaspersky Lab. (2018). *Ransomware: definición, prevención y eliminación*. Obtenido de https://latam.kaspersky.com/resource-center/threats/ransomware

KIC. (2017). "Tankyu" Practice. Kobe, Japón.

Londoño Forero, J. A. (2014). Seguridad Informática. Medellín, Colombia.

Machín Osés, N., & Gazapo Lapayese, M. (2016). La ciberseguridad como factor crítico en la seguridad de la Unión Europea. *Revista UNISCI*, 22.

Mendoza, M. Á. (2015). *¿Ciberseguridad o seguridad de la información? Aclarando la diferencia.* Obtenido de welivesecurity - ESET: https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/

MICS. (enero de 2014). *Plan Nacional de Seguridad Integral 2014-2017.* Obtenido de http://instrumentosplanificacion.senplades.gob.ec/documents/20182/22941/PlanNacionaldeSeguridadIntegral2014-2017.pdf/f60ca2ad-41d6-4c1b-9b0d-05336e548f5f

MIES. (01 de 06 de 2018). *Se firma el "Pacto con niñas, niños y adolescentes por una Internet segura"*. Obtenido de https://www.inclusion.gob.ec/se-firma-el-pacto-con-ninas-ninos-y-adolescentes-por-una-internet-segura/

MIES; MINTEL; MINEDUC. (2018). Pacto operativo del Gobierno Nacional con la Niñez y Adolescencia por un internet seguro. Quito, Pichincha, Ecuador.

MINTEL. (2018). *Motivos de visitas y capacitaciones en Infocentros*. Obtenido de https://tinyurl.com/y8pdvzko

MINTEL. (2018). *Plan Nacional de Alistamiento Digital – PLANADI*. Obtenido de https://www.telecomunicaciones.gob.ec/plan-nacional-de-alistamiento-digital-planadi/

MINTEL. (2018). *Ranking de evaluación de las entidades públicas del cumplimiento de la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).* Quito.

MINTEL. (2018). Subsecretaría de Estado de Gobierno Electrónico. *Evaluación del políticas en el sector público*. Quito.

MINTEL. (2018). Subsecretaría de Inclusión Digital. *Campañas de sensibilización sobre Seguridad de la Información y Ciberseguridad*. Ecuador.

Pastorino, C. (6 de 12 de 2017). *Convenio de Budapest: beneficios e implicaciones para la seguridad informática*. Obtenido de weliveswcuriry by ESET: https://www.welivesecurity.com/la-es/2017/12/06/convenio-budapest-beneficios-implicaciones-seguridad-informatica/

RCG Comunicaciones. (2018). *Los ciberataques: tipos y previsiones para el 2018*. Obtenido de http://rcg-comunicaciones.com/los-ciberataques-tipos-previsiones-2018/

Rodríguez, A. (18 de enero de 2016). *TrustDimension.* Obtenido de http://www.trustdimension.com/la-importancia-de-la-seguridad-informatica/

Rodríguez, G. S. (2016). *Cuestiones Jurídicas - Revista de Ciencias Juridicas de la Universidad Rafael Urdaneta*. Obtenido de Ciberseguridad realidad y tendencias en Venezuela.

Ron, M., Fuertes, W., Bonilla, M., Toulkeridis, T., & Diaz, J. (2018). Cybercrime in Ecuador, an Exploration, wichh allows to define Nacional Cybersecurity Policies. Caceres, España: IEEE.

Ron, M., Rivera, O., Fuertes, W., Toulkeridis, T., & Diaz, J. (2018). Cybersecurity Baseline, an Exploration, which allows to define National Cybersecurity Policies in Ecuador.

SENESCYT. (2018). Información sobre formación en Seguridad de la Información y/o Ciberseguridad. Quito, Ecuador.

SNAP. (2013). Acuerdo Ministerial Nro. 166. *Esquema Gubernamental de la Seguridad de la Información*. Ecuador.

UIT. (2014). *Plenipotentiary Busan Korea*. Obtenido de https://www.itu.int/en/plenipotentiary/2014/newsroom/Documents/backgrounders/pp14-backgrounder-building-trust-icts-cyberspace-es.pdf

UIT. (2015). *2030 Agenda for Sustainable Development*. Obtenido de https://www.itu.int/en/ITU-D/Statistics/Pages/intlcoop/sdgs/default.aspx

UIT. (2015). *Índice mundial de ciberseguridad y perfiles de ciberbienestar*. Obtenido de https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-S.pdf

UIT. (2017). Global Cybersecurity Index. Ginebra, Suiza.

Universidad Internacional de Valencia. (09 de septiembre de 2016). *¿Qué es la seguridad informática y cómo puede ayudarme?* Obtenido de https://www.universidadviu.es/la-seguridad-informatica-puede-ayudarme/