UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS.

ESCUELA DE RELACIONES INTERNACIONALES.

TEMA DE INVESTIGACION: CRIMENES DEL SIGLO XXI: EL IMPACTO DE LA CIBERSEGURIDAD EN LA GOBERNANZA DE COSTA RICA TOMANDO COMO BASE LOS CASOS DE MEXICO Y ESTADOS UNIDOS (2015-2019)

MODALIDAD DE TESIS PARA OPTAR POR EL GRADO DE BACHILLERATO EN RELACIONES INTERNACIONALES.

NOMBRE DEL ESTUDIANTE:
ANDREA ARAYA BOGANTES.

TUTORA DE LA INVESTIGACION:
PAMELA RAMIREZ GUEVARA.

SEDE ARANJUEZ, SAN JOSE
JULIO, 2020

AGRADECIMIENTOS

Agradezco infinitamente a mi familia, por todo el apoyo que me han dado durante la composición de este documento que culmina muchos años de trabajo, estudio y esfuerzo.

Agradezco a mis amigos: Erick y Karen, porque me han revisado, leído y corregido, siempre recordándome la luz al final del camino. Siempre positivos alrededor del avance del trabajo de investigación.

A mis amigas de la oficina: Nathy, Mary, Gaby, Mariana y Kath porque siempre me cuidaron cuando más complicado se hacia el día laboral y con una sonrisa lograron darme ánimos para continuar.

Agradezco a Dios y a mi mamá, porque siempre me han iluminado cuando no podía escribir más.

Andrea Araya Bogantes.

DEDICATORIA

A mi dulce, creativa, aventurera, desafiante y fuerte hija, a Luciana, porque ella me ha enseñado que ser mamá es un privilegio, ser mujer es maravilloso y ser profesional es una elección de vida.

Porque recordarle a ella que los sueños se cumplen y que se debe ser perseverante en un mundo cambiante es importante, y que todas las experiencias algo siempre nos deja.

Andrea Araya Bogantes.

RESUMEN EJECUTIVO

El escenario internacional se ha transformado a lo largo de la historia, no solo a nivel político y económico, pero también a nivel tecnológico. Los cambios han tenido un impacto en el Sistema y como la dinámica de este se jerarquiza. La innovación tecnológica vino a recomponer la forma en que las potencias utilizaban la diplomacia y la economía dentro de la esfera de la seguridad nacional. Los mismos organismos internacionales han tenido que evolucionar para mantenerse vigentes en el mundo interdependiente.

Es el fenómeno de la globalización el que genera presión para interconectar a los usuarios. Los servicios primarios para la sociedad, como la electricidad, transporte y banca financiera dependen en alguna medida de las TIC's, inclusive en países que no son potencias. Sin embargo, el uso indiscriminado y desregulado permite la aparición de nuevas formas de crímenes informáticos. Diariamente, las personas son blancos de los ataques cibernéticos vistos como fraude o hackeo. Es por esta razón, que conceptos como el de ciberseguridad han tomado mayor validez en el planteamiento de la seguridad nacional de un Estado.

Para comprender el impacto de la ciberseguridad, es imperativo conocer el entorno en el cual se desarrollan las políticas de seguridad nacional. Si bien en la actualidad, la preponderancia de las tecnologías de la información ha generado un cambio social, cultural y económico; los riesgos y amenazas de la utilización de estas ha sido un tema complejo de definir debido a su constante evolución. Los Estados han tenido que manejarse alrededor de las formas novedosas de delinquir aceptando una limitación del poder virtual que poseen.

Es por la conceptualización de conflictos como las Primaveras Árabes e incluso el 9/11 que los Estados modifican sus estrategias de seguridad acuñando el termino de seguridad cibernética o ciberseguridad debido a la necesidad de defensa y como une medio de protección de datos, parte de la protección de los derechos fundamentales de los individuos. Las estrategias de Seguridad Nacional Cibernética en América Latina y

en Costa Rica han fomentado un nuevo enfoque a la terminología de seguridad ciudadana. Es así, como el uso de la huella digital en la sociedad impacta la creación de las políticas públicas y la actualización de la regulación en un país desmilitarizado.

La importancia de mantener una claridad normativa alrededor de los esfuerzos de ciberseguridad es relevante para entender como la gobernabilidad se transforma en gobernanza, el accionar y la ejecución de las políticas públicas se traduce a los ámbitos sociales del país. La influencia de las TIC's, la protección de los datos y el acceso que la población tiene da un panorama completo del estado de la gobernanza para Costa Rica y ayuda a trazar los cambios para una población menos desigual.

Tabla de Contenidos

CAPÍTULO I: INTRODUCCIÓN.

El escenario internacional se ha transformado a lo largo de la historia, no solo a nivel político y económico, pero también a nivel tecnológico. Los cambios han tenido un impacto en el Sistema y como la dinámica de este se jerarquiza. Si bien, se puede hablar de un mundo occidentalizado tradicional, la innovación tecnológica vino a recomponer la forma en que las potencias utilizaban la diplomacia y la economía dentro de la esfera de la seguridad nacional. Los mismos organismos internacionales han tenido que evolucionar para mantenerse vigentes en el mundo interdependiente.

A partir del Siglo XX, la sociedad global ha ido avanzando tecnológicamente a pasos agigantados, desde las mejoras de transportes, el auge en la cooperación comercial y los avances en comunicación por mencionar algunos. En la actualidad, el fenómeno de globalización es tan intrínseco en la vida cotidiana que muchas personas ni siquiera se preguntan que existió previo a la tecnología utilizada día a día. Avances en la World Wide Web, los usos computacionales y la constante innovación del ciberespacio nos han dejado una visión interdependiente de cómo nos relacionamos.

Es por estos avances que el Sistema Internacional, lo cual se entiende como las interacciones entre Estados, organismos internacionales y empresas transnacionales, se ha alterado. Ahora se debe tener en cuenta el empoderamiento que se le ha brindado a los individuos en la participación de los asuntos estatales. A mayor transparencia y agilidad en este sentido, mayor democracia. Queda claro que el marco jurídico en que estos ejes se manejan también se ha reformado, aunque no necesariamente con la rapidez en que la tecnología innova.

Las tecnologías de información y comunicación (TIC’s) han surgido de los métodos de correspondencia, como código morse, telégrafo y después el teléfono, logrando la conexión interoceánica. Son métodos como las computadoras, los teléfonos celulares y las redes de datos los que han logrado interconectar a toda la población, forjando una sociedad de la información, y su alcance es medido continuamente, pues es parte de la visión de un mundo globalizado. El uso del internet ha hecho que las TIC’s

sean omnipresentes y que la digitalización de los Estados y del sector privado tenga altas demandas.

Es el fenómeno de la globalización el que genera presión para interconectar a los usuarios, de tal manera que la integración de la tecnología en productos como carros o edificios es ahora posible. Los servicios primarios para la sociedad, como la electricidad, transporte y banca financiera dependen en alguna medida de las TIC's, inclusive en países que no son potencias. Los beneficios para los países en vías de desarrollo van de la mano con la oferta y demanda del uso de la información, pues la economía ha forzado al mercado a ofrecer los servicios a menores costos. De esta forma se da una mayor oportunidad de interconectarse comprando por ejemplo un teléfono celular con acceso a internet por un menor costo.

La influencia de las TIC's se ejemplifica en el uso de correo electrónico para comunicarse, o la presencia de empresas transnacionales en el mundo cibernético para atraer mayor cantidad de clientes. Pero de igual forma, se pueden utilizar para llegar a áreas remotas y ser usadas como herramienta para el progreso, especialmente en el combate de la reducción de la pobreza. El esfuerzo global entonces está generando estrategias de inmersión estatales de las TIC's para tratar de aumentar la productividad y habilitar el acceso de los servicios básicos.

Sin embargo, el uso indiscriminado y desregulado permite la aparición de nuevas formas de crímenes informáticos. Diariamente, las personas son blancos de los ataques cibernéticos vistos como fraude o hackeo. El cibercrimen afecta sectores productivos de la sociedad, en su mayoría, las entidades financieras son apetecidas debido a la información que manejan. También, debido a la obtención de capitales de las personas que logran estafar. Es por esta razón, que conceptos como el de ciberseguridad han tomado mayor validez en el planteamiento de la seguridad nacional de un Estado.

Ahora el desarrollo de políticas de ciberseguridad debe formar parte de las preocupaciones de las administraciones, pues también es un indicador de bienestar estatal. La protección del ciberespacio y de sus usuarios es un campo de desarrollo del

cual se deben ocupar las políticas públicas. Como se indicará en la presente investigación, la cooperación interestatal y el papel que juegan las potencias como innovadores de procesos y regulación cibernéticas presentan un impacto directo en la gobernanza de los Estados.

La implementación de medidas de protección es importante para los Estados pues no solo se limita a la legislación. También es relevante la concientización desde el ámbito educativo de los usuarios pues el impulso de hacia la generación de ciudadanos digitales empoderados para trabajar con las nuevas tecnologías. Los proyectos de ciudades digitales a su vez incentivan el compromiso y apertura de las administraciones al reconocer la importancia de la tecnología en la cotidianidad.

El manejo responsable de las distintas amenazas del cibercrimen representa un desafío por sí solo. No solamente porque la estrategia debe tener medidas jurídicas actuales sino puesto que se requieren avances técnicos que permiten garantizar la ciberseguridad. Estos avances a su vez significan un elevado costo de manutención estatal, costos que algunos Estados tienen dificultad para incluir a nivel presupuestario. Sin embargo, los riesgos asociados a bajos niveles de protección pueden llegar a afectar a los usuarios, las empresas y al mismo Gobierno.

La responsabilidad asociada a la ciberseguridad debe comprender el compromiso estatal, de las organizaciones internacionales y del individuo. Es por lo que definir el impacto que los distintos ataques cibernéticos tienen sobre la sociedad, consta de diferentes variables. El rol de las Relaciones Internacionales en este contexto prueba que la interconexión entre los distintos sectores como la economía, la gobernabilidad y la tecnología son aspectos de estudio constante.

La importancia de mantener una claridad normativa alrededor de los esfuerzos de ciberseguridad es relevante para entender como la gobernabilidad se transforma en gobernanza, el accionar y la ejecución de las políticas públicas se traduce a los ámbitos sociales del país. La influencia de las TIC’s, la protección de los datos y el acceso que la

población tiene da un panorama completo del estado de la gobernanza para Costa Rica y ayuda a trazar los cambios para una población menos desigual.

El presente trabajo investigativo pretende esclarecer la situación de Costa Rica frente a estos desafíos y como se piensa incentivar el uso de recursos tecnológicos de forma adecuada. Es inherente para este estudio la constatación que la globalización y la ciberseguridad están generando una nueva sociedad de la información, donde la adaptabilidad del Sistema Internacional influye directamente en los individuos.

1.1 Planteamiento del Problema

Las tecnologías de la información y comunicación (TIC's) son parte inherente de la Sociedad de la Información. Su principal propósito ha sido el de proveer de herramientas científicas al mundo para comunicarse con mayor facilidad. Esta idea incluye infraestructura de telecomunicaciones robusta, auge en la cooperación interinstitucional, agilidad interestatal y principalmente, en la actualidad, un mejor y mayor flujo económico que potencie el desarrollo de los Estados y las entidades privadas.

Sin embargo, no se pensaba que las TIC's iban a llegar a tener un papel relevante en los temas de seguridad nacional y que se desarrollara todo un sector relacionado a la protección de los datos que se encuentran en la red. El auge exponencial del cibercrimen, que promedia 0,5% del PIB mundial en 2016 (Parraguez Kobek, 2017), deja entrever la situación que atraviesan los Estados. Por un lado, la mejora de la conectividad de su población y los beneficios que se derivan; y paralelamente la necesidad de generar políticas públicas que resguarden la información estatal y privada de las mismas.

La creación de políticas de mejoramiento del desarrollo tecnológico regionales se ha acompañado de aquellas que tengan la ciberseguridad como pilar. Algunos actores internacionales como Estados Unidos de América han enfocado su estrategia en salvaguardar su patrimonio nacional por medio de políticas de seguridad nacional, que devengan hasta $109 billones de dólares de su presupuesto anual (The Council of Economic Advisers, 2018). Teniendo en cuenta actividades cibernéticas maliciosas que

comprenden desde ataques de servicios, destrucción de datos, ruptura de comercios y robo de propiedad intelectual se lleva una revisión de las llamadas infraestructuras críticas y el desarrollo de una estrategia nacional de ciberseguridad.

Otros actores, como México, han desarrollado estrategias entorno a la necesidad de protección a la sociedad mexicana, facilitando espacios de dialogo y tomándoles en cuenta para desarrollar las políticas estatales. La estrategia nacional mexicana se enfoca en la perspectiva que el ciberespacio es parte del escenario global y por lo tanto debe entenderse que el esfuerzo para que la seguridad en el ciberespacio se cumpla se debe tener cooperación entre los actores nacionales e internacionales para llegar a acuerdos conjuntos sobre las amenazas y los ciberdelitos.

De esta manera, se observa que el nivel de desarrollo de políticas en los diferentes Estados de la región varía, desde aquellos que adjudican tiempo para la creación de legislación acorde a los cambios tecnológicos para salvaguardar la seguridad nacional y otros se encuentran en un proceso de reconocimiento que permita la atención estatal ante ciberataques. En el caso de Costa Rica, la legislación que interconecta al gobierno con la Estrategia Nacional de la Ciberseguridad se concentra en el mejoramiento de la infraestructura y la conectividad de las instituciones públicas por medio del Gobierno Digital. Así como la penalización de los delitos cibernéticos, únicamente definidos acorde en la normativa jurídica, dejando un amplio espectro de posibilidades para los nuevos tipos de crimen.

La incipiente investigación e interacción gubernamental con respecto a la seguridad de las TIC’s deja un vacío que consiste en uno de los problemas planteados en la investigación. Si bien, el Estado costarricense se encuentra en la posición 44 del Índice de Conectividad, y el peso de las exportaciones de bienes TIC representa alrededor de 41% (Ministerio de Ciencia, Tecnología y Telecomunicaciones, 2017), no se cuenta con la legislación adecuada que regule las instituciones estatales frente al cibercrimen y aún más, deja una apertura clara a ataques que podrían afectar de manera severa la seguridad de todos los costarricenses poniendo riesgos a nivel social, económico y diplomático.

Mientras que las potencias occidentales facilitan presupuesto a la seguridad nacional enfatizada en la protección del ciberespacio, frente a su potencial riesgo de altercados con países como Corea del Norte y China. Estos Estados adjudican a los departamentos encargados de la seguridad la responsabilidad directa de mantener la infraestructura critica para poder responder ante ataques, así como empoderarlos para que adquieran el nivel adecuado de ciberseguridad. De esta manera, el presupuesto asignado a las entidades estatales se traduce alrededor de 100 billones de dólares (The Council of Economic Advisers, 2018) dando la capacidad a estas instituciones de alertar a compañías que sufren de vulnerabilidades o ciberataques sin detectarlo, desde robo de datos hasta decomiso de infraestructura.

En Costa Rica, al tener deficiencias en el sector legislativo, esto se traduce directamente a una dificultad de ejecución y protección del Estado por parte de las entidades correspondientes: el Centro de Respuesta a Incidentes de Seguridad Informática (CSIRT-CR). Mientras que, se espera que el CSIRT-CR busque la implementación y gestión de medidas para mitigar el riesgo de ciberataques; también el Ministerio de Ciencia, Tecnología y Telecomunicaciones (2017) le da la tarea de incorporar el sistema de seguridad para el Gobierno Central y sus diferentes entidades. Con un departamento que carece de recursos presupuestarios, el alcance de la entidad se reduce a capacitaciones sobre ciberseguridad, ocasionando una problemática directa al bienestar a nivel cibernético del Estado y sus habitantes.

Esta problemática representa una vulnerabilidad para el Estado y para entidades privadas dentro de nuestro territorio, como lo indica el diario Semanario Universidad (2019) fueron 19 millones de ataques de diversos indoles cibernéticos que sufrió Costa Rica el año anterior concentradas en entidades financieras y gubernamentales. Dentro del CSIRT-CR son únicamente cuatro ingenieros informáticos quienes deben redireccionar y mitigar perdidas a nivel costarricense; luchando con una situación económica, que en este caso compite con otros escenarios que preocupan y generan más presión al Gobierno Central.

Una tercera problemática, se refiere a la especialización que se requiere para poder desarrollar de manera estratégica las TIC's y la seguridad cibernética. Mientras que la ingeniería especializada en seguridad cibernética toma relevancia en el mundo y las necesidades dentro del ciberespacio aumentan son pocos países como China y Estados Unidos quienes logran egresar una mayor cantidad de especialistas que lleguen a puestos de empresas privadas o instituciones estatales. De igual manera, en los últimos años se ha presentado una baja en los costos asociados a la conectividad y el desarrollo de software facilitando la exportación de servicios, pero generando un déficit de especialistas en el sector de alrededor de una proyección de 3.5 millones de profesionales (Cancino, 2020).

La formación académica históricamente ha obtenido alrededor del 8% del PIB en Costa Rica (Ministerio de Ciencia, Tecnología y Telecomunicaciones, 2017), pero de esto la mayoría se concentra en mejoras en la infraestructura y procesos de enseñanza. La oferta académica especializada en Costa Rica ha aumentado, sin embargo, el país cuenta con un déficit de especialistas en seguridad informática que para el CSIRT-CR implica falta de personal para el manejo de vulnerabilidades, y en el sector privado implica una dificultad para poder reaccionar apropiadamente frente a ataques directos de cualquier tipo. En 2018 el Semanario Universidad dejo entrever que el MICITT había autorizado tres plazas para el CSIRT-CR, que no fueron cubiertas por la falta de personal calificado. Aunque la legislación promocione el mejoramiento de la infraestructura en las instituciones públicas la idea de robustecer la seguridad informática con un déficit de personal para más de 300 instituciones públicas genera retos que no podrían ser sobrepasados con la falta de especialistas actual.

Es por ello por lo que la pregunta fundamental de esta investigación es: ¿Cuál es el impacto de la ciberseguridad en la gobernanza de Costa Rica?

1.2 Objetivos

En la presente investigación se tratará de esclarecer la situación de la ciberseguridad en Costa Rica, por tanto, se pretende tomar distintos objetivos que componen en su la forma en la que se está gobernando el ciberespacio costarricense.

1.2.1. Objetivo General

Estudiar el efecto de la ciberseguridad en las políticas de seguridad que afectan la gobernanza de Costa Rica.

1.2.2 Objetivos Específicos

En cuanto a los objetivos específicos para la investigación, se pretende:

1. Reconocer la evolución de los desafíos relacionados a las Tecnologías de la Información.
2. Describir las políticas de seguridad nacional que utilizan Estados Unidos y México en cuanto a ciberseguridad.
3. Identificar el estado de la gobernabilidad en Costa Rica en torno a la legislación de las tecnologías de seguridad de la información.
4. Analizar el impacto de la ciberseguridad en la gobernanza.

1.3 Justificación

Con el acceso a las tecnologías de la información en los diferentes sectores económicos y sociales, los crímenes tecnológicos han tenido un espacio en el cual se da disponibilidad para atacar la privacidad de los ciudadanos, las interacciones en el sector privado y público de un Estado. Es por ello por lo que la generación de nueva legislación que lograse generar defensa toma relevancia. Los Estados y las organizaciones interestatales no se encuentran capacitadas para responder de manera adecuada ante los riesgos, al menos cuatro de cinco países en la región no tienen una estrategia de ciberseguridad (PROSIC, 2010) que garantice la protección de la infraestructura critica. Inicialmente porque lo que se definía como cibercrimen tomaba como base los delitos tradicionales, desde el modo en que se cometía el crimen hasta el asalto de los bienes jurídicos

Con el tiempo, países como Estados Unidos han logrado desarrollar una estrategia que comprende directamente la seguridad nacional, la defensa de la economía estatal y la protección de los ciudadanos como consumidores de tecnología. Pero este no es el panorama de toda la región, donde los esfuerzos jurídicos apenas empiezan y donde las distintas estrategias no obedecen a un marco común para presionar a los depredadores virtuales.

La generación de políticas acorde a la variedad terminológica y oportunista de los crímenes cibernéticos se vislumbra como uno de los desafíos más grandes para una región en crecimiento tecnológico. En el país, según el MICITT en la Estrategia Nacional de Ciberseguridad (2017) el sector de telecomunicaciones y exportación de servicios relacionados a las TIC’s representaba para el 2015 un 6,8% del PIB, y las expectativas económicas indican que el sector seguirá en crecimiento permitiendo mayor cantidad de amenazas cibernéticas.

Es por esto por lo que el análisis del estado actual de la ciberseguridad en Costa Rica cobra relevancia para la gobernanza de este. No se habla solo de la necesidad de presentar un marco jurídico que permita el desarrollo de los ciudadanos virtuales, sino

que, a partir de esto, que sea el Estado en conjunto con otras organizaciones internacionales, los que garanticen la protección frente a ataques informáticos de terceros. El pilar económico que representan las TIC's para Costa Rica en si debiera ser suficiente, según opinión propia, para que el Estado encuentre formas de gobernar adecuadamente en el ciberespacio.

Las TIC's al ser un catalizador de desarrollo permiten que la sociedad se interconecte, y la Estrategia Nacional (2017) pretende centrarse en las personas que utilizan de la tecnología con la responsabilidad compartida del uso de dispositivos y redes con el Estado. Es por esta razón, que la ciberseguridad se torna en un tema educativo y cultural pivote de los comportamientos sociales costarricenses. Lograr que un ciudadano promedio reconozca la importancia de la ciberseguridad en su vida cotidiana, así como la relevancia para la protección de datos y el rol que juega el Gobierno en la toma de las decisiones alrededor del cibercrimen es nuestro nuevo paradigma como sociedad.

Que el Estado costarricense reconozca la importancia de lo anterior, dentro del marco de los derechos humanos relacionados al acceso de información y respeto de la privacidad debe ser de relevancia pública. En algunos países como México y Costa Rica se encuentran en la búsqueda de las formas apropiadas institucionales para equilibrar el desarrollo tecnológico y la correlación que la promoción de las TIC's tiene en los distintos sectores. Este último punto se relaciona con el gasto tanto público y privado que se debe mantener para asegurar la seguridad cibernética.

Además, el proyecto de investigación es la base analítica que permite tener una perspectiva en aspectos jurídicos y educativos sobre el estado de relevancia para el Estado alrededor de la ciberseguridad. Todos tenemos acceso gracias a la globalización de la información, pero también somos permeables en cuanto a daños sobre nuestros datos. Desde acceso a cuentas bancarias hasta alteración de registros médicos para los ciudadanos, y para los Estados, alteración de los servicios u operaciones de las entidades gubernamentales. Es por esta razón, que aprender e interiorizar la situación pública sobre la seguridad de la información en las políticas públicas debe ser

transparente y coordinada con otros actores. Los ciudadanos costarricenses deber ser resilientes para enfrentar ciberataques.

Con la investigación, se expone la necesidad en la sociedad costarricense para apoyar de forma más inclusiva las especializaciones académicas, y que esto se traduzca en oportunidades de mejorar la infraestructura critica, la coordinación tecnológica de las entidades públicas y la cooperación con el sector privado. Asimismo, la forma de legislar los nuevos ámbitos tecnológicos globales deja un sector desprotegido que debe ser atendido por los Estados y ONG's. Es un esfuerzo conjunto para la seguridad internacional lograr un mejor equilibrio que alcance las nuevas formas de atacar, tanto a las personas como los Estados que podría potencialmente generar un desbalance a nivel económico y social.

El continuo uso de la web para el desarrollo de diferentes capacidades expone la necesidad de la detección temprana y combate efectivo de los ciberataques. Se plantea que, con la resiliencia, o ciberresilencia se transforme en una necesidad inherente a la sociedad global. En donde todos los ámbitos públicos y privados deben de estar alineados entorno a la transparencia y facilidad de manejo de la tecnología para tratar de solventar crímenes que se divisan como anónimos. Hay que reconocer que las mismas innovaciones pueden ser utilizadas en beneficio o perjuicio de la sociedad, si esta no las entiende y las usa de forma racional o conveniente.

Cuantificar el impacto de los distintos tipos de ataques que crean efectos físicos, manipulan, interrumpen o eliminan datos en la economía e infraestructura digital de un Estado, es relevante para países como Costa Rica cuyo presupuesto tiene un rubro específico para inversión extranjera directa y sus alcances (Ministerio de Ciencia, Tecnología y Telecomunicaciones, 2017). De igual manera, las propuestas de la Estrategia Nacional de Ciberseguridad tienen impacto a nivel educativo, judicial y de los servicios para la regulación y estabilización de la ciberseguridad en Costa Rica. Cabe recalcar que la administración de las políticas de seguridad cibernética, al menos, están pautadas dentro del actual marco jurídico.

El desarrollo de las variables de la investigación provee un escenario de la gobernanza costarricense en el nivel tecnológico y de seguridad el cual cobra importancia la exposición del Estado a nivel internacional. A su vez, se determina que tanto los ciudadanos entienden la importancia de proteger los datos privados, para evitar actividades maliciosas en detrimento de desarrollo como sociedad. La exploración de la metodología en este caso aporta a investigaciones futuras el uso de las fuentes primarias ligadas a los diferentes enfoques que los Estados en la actualidad tienen con respecto al Sistema Internacional.

1.4 Antecedentes

Los antecedentes investigativos relacionados a la ciberseguridad como parte de la gobernanza de un Estado no han sido correlacionados previamente. Aunque se investigan la ciberseguridad como estrategia nacional, o la necesidad de una estrategia que tenga un contexto humanístico no existe un estudio de impacto en la gobernanza de un país. Por lo tanto, se utiliza como investigaciones previas la Estrategia Nacional de Ciberseguridad de Costa Rica, de México y de Estados Unidos.

Según la Estrategia Nacional de Ciberseguridad (2017), el Ministerio de Ciencia, Tecnología y Telecomunicaciones de Costa Rica es el ente encargado del desarrollo de las políticas públicas relacionadas al sector de telecomunicaciones y la Superintendencia de Telecomunicaciones (SUTEL) es la encargada de la regulación de las mismas. Desde el 2005, el gobierno ha empezado a desarrollar ciertos precedentes que crean una base alrededor de la seguridad de las tecnologías de la información, específicamente con la creación de la Ley 8454 (Ley de Certificados, Firmas Digitales y Documentos Electrónicos) en donde se identifica la necesidad estatal de reconocer la validez de los documentos digitales en comparación con los físicos y su utilización en las distintas entidades públicas o privadas.

Adicionalmente, en la Ley 8454, se determina la importancia de la creación de certificaciones digitales y la administración de estas para el uso interno y externo en los casos de vinculación jurídica, autenticación y no alteración de documentos que en

conjunto con la firma digital demuestren autoría de estos (La Gaceta, 2005). Este acto responsabiliza a las personas de tal manera que el Estado evita el anonimato en las transacciones y demuestra con claridad los alcances que se le puede dar al uso de las tecnologías de la información; siendo uno de los primeros pasos para posteriormente indicar las políticas que consideran la seguridad de la información.

En el 2010, el Reglamento sobre Medidas de Protección de la Privacidad de las Comunicaciones viene a cubrir lo dispuesto en la Ley 8642 (Ley General de Telecomunicaciones) que integra la relación entre los operadores de redes públicas o proveedores de servicios de telecomunicaciones y el Estado, fomentando la corresponsabilidad en la protección de la privacidad de los usuarios, el secreto de las comunicaciones, el derecho a la intimidad y las limitantes del tráfico o localización de datos. Asimismo, garantiza que la seguridad de las redes debe estar establecida por las entidades que proveen estos servicios y que la SUTEL, como ente regulador, debe dar cuentas a los ciudadanos del uso correcto de la información privada.

Otros pilares en la construcción de la infraestructura alrededor de la seguridad tecnológica se refieren a la creación de entidades gubernamentales como la Agencia de Protección de Datos de los Habitantes (PRODHAB), en el 2011, que se encarga de según el Ministerio de Ciencia, Tecnología y Telecomunicaciones (2017) de “garantizar el respeto a la autodeterminación informativa en el tratamiento de los datos de su persona o bienes” específicamente. Se trata de una entidad que ayuda de manera paralela a otras instituciones gubernamentales en la agilización de datos, control y protección. Ante la PRODHAB también se pueden presentar denuncias en el espacio de la cibernético que judicialmente carecían de respuesta.

La base fundamental para la Estrategia Nacional de Ciberseguridad se diseñó en el 2012, en forma de la Ley de Delitos Informáticos que regula ampliamente el estado de los crímenes cibernéticos y los describe en cuanto a alcance regulatorio penal. Esta ley cabe recalcar tuvo que ser modificada, pues la manipulación informática no estaba contenida en la misma. Es por esta razón que constituye el pilar para la regulación jurídica costarricense en cuanto a delitos de tecnologías de información como espionaje,

extorsión, daño informático, instalación del malware, entre otros. Mas recientemente, a nivel internacional, el Estado costarricense ha tratado de mejorar el marco normativo firmando el decreto para el proceso de adhesión de la Convención sobre el Cibercrimen, en el 2017, que actúa de manera directa sobre la temática de los delitos informáticos detallada inicialmente.

Las tecnologías de la información se han desarrollado acorde a la oferta y demanda, por ello la innovación y su crecimiento acelerado ha tenido un impacto directo en la manera que el Sistema Internacional se desenvuelve. Desde escenarios de infraestructura física, como mejoras en las vías de tránsito, hasta la revolución digital, con la simplificación de transacciones e interdependencia de las acciones en la web: personificación digital, proveeduría de datos personales, agilización de servicios gubernamentales. Esto significa que los Estados han tenido que generar estrategias tanto para estimular la penetración de las TIC's en la sociedad y en la infraestructura de redes de los gobiernos locales.

De igual forma, el auge de las TIC's ha traído en el Sistema Internacional consecuencias que presentan a los Estados y otros actores situaciones maliciosas para el control de datos y que se tengan que desarrollar estrategias de control de un espacio cibernético que aún no se conoce completamente su alcance. Esta posibilidad, seria, en definitiva, en detrimento de la economía mundial y subsecuentemente tendría un impacto en otras áreas relativas a la población. Los Estados han empezado a trabajar distintas propuestas para poder continuar con la visión de ciberseguridad que ha sido capitalizada a partir de casos de terrorismo en el mundo Occidental.

La Estrategia Nacional de Ciberseguridad (2017) tiene como objetivo general "desarrollar un marco de orientación para las acciones del país en materia de seguridad en el uso de las TIC, fomentando la coordinación y cooperación de las múltiples partes interesadas y promoviendo medidas de educación, prevención y mitigación frente a los riesgos en cuanto al uso de las TIC para lograr un entorno más seguro y confiable para todos los habitantes del país" es por ello que viene a convertirse en el pilar actual para los procedimientos frente a la comunidad internacional en cuanto a resguardo y medidas

de protección sobre los datos. Casualmente, sentando un precedente en la región que está en los inicios de esfuerzos sobre la medición del impacto y protección de las TIC's

Esta estrategia plantea que el desarrollo de las TIC en sectores como salud, seguridad ciudadana, educación, cultura, comercio y gobierno digital si bien mejora los indicadores de acceso y uso de las tecnologías no necesariamente desarrolla un plan específico sobre la protección de los datos. Es por esta razón que la estrategia consta con un instrumento en donde se refiere al Plan Nacional de Desarrollo de las Telecomunicaciones, en donde se propone transformar al país en una sociedad en el ciberespacio, Modelo de Ciudades Digitales, pero con protocolos en Ciberseguridad en el Gobierno Central, así como un lineamiento a nivel nacional como base para el resguardo cibernético.

También, esta misma estrategia plantea los avances de los proyectos en las distintas áreas; en el sector salud por ejemplo la implementación del Expediente Digital Único de Salud (EDUS) utilizado por la Caja Costarricense del Seguro Social. En el Ministerio de Seguridad Publica se desarrolla la plataforma en línea para registro de agentes y empresas de seguridad. La automatización de tramites es un esfuerzo conjunto en donde se destaca la Ventanilla Electrónica de Servicios (VES) y el Sistema de Compras Públicas (SICOP). Todos estos proyectos incentivan la digitalización de información y es donde los lineamientos de ciberseguridad cobran relevancia debido al impacto que tendría un posible ataque a los datos contenidos en la red del gobierno.

Se ha comentado la conexión del desarrollo de las TIC's y su protección en Costa Rica con la cooperación entre Estados. La Estrategia Nacional de Ciberseguridad de México establece puntos en común con la costarricense en cuanto a la importancia de las TIC para el desarrollo sectorial: político, económico y social al brindar mayor conectividad tanto para los individuos como para las organizaciones públicas y privadas. Asimismo, los riesgos asociados por causa de los ciberdelitos y la necesidad de una estrategia de ciberseguridad. La estrategia da una referencia al desarrollo de políticas propias para cada estado y su capacidad económica, teniendo en cuenta que la región tiene distintos grados de avance.

Para México es importante tener en cuenta el costo económico aproximado, 3000 millones de dólares (Estado de México, 2017), que se ha utilizado para el combate de cibercrímenes y el desarrollo de una política sostenible que tenga en cuenta los derechos humanos, gestión de riesgos y colaboración de los diversos actores. Las distintas fases de la Estrategia Nacional han tenido como finalidad la digitalización en donde se expone la brecha digital de protección al no tener una Agencia de Ciberseguridad Nacional que incentive la gobernanza digital, definición de un marco jurídico que tenga en cuenta leyes federales y estatales y protección de infraestructura critica. Este último punto es una debilidad que el Estado costarricense comparte y debe de tener en cuenta también en la creación de políticas públicas.

Cabe recalcar que la Estrategia Nacional de Ciberseguridad de México (2017) es un planteamiento inicial del estado de las TIC's y la visualización del futuro en la institucionalización de la protección de datos. Inicialmente concentrado en distintos ejes que aumenten el uso de las tecnologías de la información, y después en el resguardo jurídico y estructural de las mismas. Con un impacto desde la base de la sociedad mexicana, hasta los actores públicos y privados que incentivan el comercio tecnológico.

Al igual que en la región, el crecimiento del uso y acceso de las TIC ha permitido al gobierno mexicano incentivar los sistemas digitales para transacciones variadas; desde logística hasta usos bancarios, que benefician a su población y logra proveer mejores servicios a menores costos (COMEXI, 2018). Los riesgos asociados también han aumentado, y es por ello que diversos organismos del gobierno deben implementar lo que COMEXI llama "iniciativas de ciberresilencia". En el 2017, no solo se crearon entidades gubernamentales, sino que también se creó la Estrategia Nacional en Materia de Ciberseguridad específica para el sector financiero.

Un caso extremo, opuesto a Costa Rica, es el de Estados Unidos. El gobierno estadounidense es pionero en la seguridad nacional y cibernética debido a su posición con respecto a los distintos actores internacionales. La ciberseguridad en Estados Unidos forma parte de la visión del gobierno para el desarrollo seguro en el ciberespacio, ya que la sociedad estadounidense es altamente dependiente de las tecnologías de la

información. Es por ello por lo que la Estrategia Nacional Cibernética (2018) se enfoca en como Estados Unidos va a asegurar a su población los beneficios de un espacio seguro en el mundo digital. Desde la perspectiva del gobierno, el impacto financiero, social, gubernamental y político que tienen las tecnologías de la información es evidente frente a la estrategia de los competidores directos que usan el ciberespacio para controlar a sus pobladores y realizar espionaje económico y ciberactividades maliciosas que ocasionan problemas a los individuos y los comercios alrededor del mundo.

La cooperación forma un pilar fundamental en la Estrategia Nacional Cibernética estadounidense, pues el Estado reconoce que cualquier cambio en la manera de atacar el problema de las tecnologías de la información debe ser de la mano del sector privado fomentando la ciberresiliencia. De igual manera, Estados Unidos indica que es necesario utilizar sanciones económicas a aquellos actores que realicen actividades maliciosas que se consideren cibercrímenes. El fomento económico interno para el mantenimiento de la infraestructura crítica y el manejo de posibles situaciones de peligro; permite al gobierno federal ocuparse de adversarios estratégicos que continúan desarrollando nuevas formas de ciberataques.

Dentro de los pilares que desarrolla la Estrategia Nacional Cibernética (2018) se proyecta primero, la protección del pueblo estadounidense, la seguridad nacional y la forma de vida de la sociedad; un segundo punto para promover la prosperidad; un tercer punto, preservar la paz por medio de la fuerza y por último el crecimiento de la influencia estadounidense. En cuanto al primer pilar, se refiere a asegurar las redes federales y la información que estas contienen, y de esta forma disminuir el ciberriesgo relacionado a la infraestructura critica que se maneja en conjunto con el sector privado. En el esquema estadounidense implica la defensa directa de la democracia. En este rubro, se incluye la inversión en ciberseguridad e innovación para tutelar tecnologías emergentes.

En el segundo pilar, se enfoca directamente en el impacto de la economía digital en el gobierno y en el potencial impulso que este esfuerzo le da al sector privado. Alineado con el primer pilar, se trata de incentivar la innovación del mercado con políticas de seguridad nacional que garanticen el cuidado de los recursos. Como efecto en

cascada, que la innovación continúe posicionando a Estados Unidos en el liderazgo de tecnologías e infraestructura que conlleve a una economía circular alrededor de las tecnologías de la información. Junto con la propuesta se debe desarrollar talento humano para que puedan manejar los cambios de manera ágil y razonable. Incentivar al sector educativo vendría a consolidar el impacto de la ciberseguridad y la calidad de los profesionales que sería reconocida a nivel mundial.

En el tercer pilar, la responsabilidad que recae en las potencias se evidencia en cuanto a la creación de marcos normativos que ayuden a regular el ciberespacio dentro del derecho internacional. Estados Unidos tiene claro que el esfuerzo no es solo a nivel estatal, sin embargo, no puede obligar a otros Estados a adherirse a una normativa que los responsabilice por el uso inadecuado de las TIC's. El cuarto pilar, resuelve sobre la integración de los derechos humanos como la libertad de expresión y el derecho a la privacidad a las amenazas cibernéticas y el rol de Estados Unidos en mantener en la lucha para ofrecer Internet de manera segura.

1.5 Proyecciones

Según la presente investigación, se pretende estudiar el efecto de la ciberseguridad en las políticas que ha desarrollado Costa Rica y su impacto en la gobernanza del país. Es por ello que se deben esclarecer los puntos fundamentales para entender el contexto actual de la seguridad en torno a las tecnologías de la información y como se vislumbra el impacto en otros sectores productivos de un país.

1.5.1 Alcances

Las tecnologías de la información tienen un impacto directo en la sociedad, y en como esta ha evolucionado en los últimos años haciendo que los individuos sean dependientes de los datos que se manejan. Es por ello, que los Estados reconocen que para el desarrollo de las TIC's deben funcionar de forma paralela iniciativas que fomenten y sensibilicen a la población. Aunado a progreso sectorial en infraestructura, educación y transparencia con la ciudadanía que garantizan a una conducción adecuada de la seguridad cibernética.

Así como el análisis de las TIC's, informa el estado de penetración sobre la ciberseguridad; ya que ambos temas se correlacionan; se debe recalcar que la transición de problemáticas sociales es transferible al ciberespacio. Es por ello por lo que, describir la desigualdad social transformada en brecha digital cobra relevancia en el entendimiento de la seguridad cibernética como un reto para el país. Comprender que observa la población en tecnología y seguridad se vuelve una consecuencia primordial del accionar del Estado en el tema.

La especialización en ciberseguridad hace que los incentivos estatales sean de gran importancia pues las tecnologías emergentes se posicionan como un riesgo potencial sino se conoce o se administran adecuadamente. Aumentar la cooperación con el sector privado, mejorar la calidad de especialistas en el sector público es necesario para generar un impacto holístico en el país.

Asimismo, la creación de un marco jurídico en el contexto global y estatal personifica los posibles delitos en el ciberespacio que cada país tiene como instrumento para el combate ante amenazas. La comprensión de cada Estado en este aspecto debe tenerse en cuenta en el momento que se compara el crecimiento de estos en el tema investigado. Se evidencia la progresividad que se le debe otorgar a la temática para poder gobernar para en el ciberespacio también.

1.5.2 Limitaciones

La presente investigación no procederá a tomar en cuenta los programas educativos que indican el abordaje del uso de TIC's en las distintas áreas de Costa Rica a menos que sean los programas especializados. Los datos para la CEPAL indican que existen desafíos en la región en las que nuestro país no está exento. Se extiende la profundidad educativa más allá del objetivo fundamental de la investigación.

Si bien, la cooperación con el sector privado es relevante para la innovación tecnológica, este enfoque se encuentra fuera del alcance de la ciberseguridad dentro de la gobernanza del país. El marco jurídico diseñado para Costa Rica se enfoca en 3 áreas: telecomunicaciones, personalidad cibernética jurídica y ciberseguridad, por ello el

impacto comercial de la empresa privada no comprende en un pilar de análisis de la acción estatal costarricense.

Otro punto que no formara parte de la investigación es el análisis comparativo de la seguridad nacional definido por México y Estados Unidos. El enfoque que se utilizara es la visión de ambos Estados en la formulación de marco jurídico interno e impacto de la Estrategia Nacional de Ciberseguridad. Esto implica un análisis concentrado en los puntos en común de las perspectivas estatales, sin mencionar la falta de tecnicidad en la estrategia estadounidense.

La comparación con México y Estados Unidos es utilizada para formar un panorama regional que permita la revisión de las políticas locales. Sin embargo, los modelos de cooperación estadounidense o los procesos económicos en la asignación de recursos militares no se amplían en la investigación.

CAPÍTULO II: MARCO TEÓRICO

Para comprender el impacto de la ciberseguridad en un Estado, es imperativo conocer el entorno en el cual se desarrollan las políticas de seguridad nacional. Si bien en la actualidad, la preponderancia de las tecnologías de la información ha generado un cambio social, cultural y económico; los riesgos y amenazas de la utilización de estas ha sido un tema complejo de definir debido a su constante evolución. Los delitos cibernéticos han ido cambiando de acuerdo con la evolución de la Sociedad de la Información y las formas novedosas de delinquir de nuevos actores y los Estados han tenido que manejarse alrededor de ellos aceptando una limitación del poder virtual que poseen.

Las sociedades digitales juegan un papel relevante en la creación del nuevo imaginario colectivo, que representa la fragmentación de la realidad. El desarrollo del ciberespacio no solo es parte de las sociedades digitales, sino que también llega a ser un espacio nuevo de conquista para el poder de los Estados. En él se ha visto un crecimiento de estrategias militares para el alcance de objetivos sobre conflictos específicos, desde las Primaveras Árabes hasta los eventos del 9/11. Es por ello que este fenómeno altera la perspectiva sobre la guerra hibrida y la guerra de la información.

Es por la conceptualización de este tipo de guerras que los Estados modifican sus estrategias de seguridad acuñando el termino de seguridad cibernética o ciberseguridad debido a la necesidad de defensa y como une medio de protección de datos, parte de la protección de los derechos fundamentales de los individuos. Las estrategias de Seguridad Nacional Cibernética en América Latina y en Costa Rica han fomentado un nuevo enfoque a la terminología de seguridad ciudadana. Es así, como el uso de la huella digital en la sociedad impacta la creación de las políticas públicas y la actualización de la regulación en un país desmilitarizado.

En un mundo fragmentado, donde la posición de los Estados ha debido cambiar; queda claro que la forma en que estos trabajan también ha sido modificada. Las comunidades digitales generan crecimiento económico, social y cultural en plataformas

tecnológicas. El Estado ha de garantizar el resguardo en el ciberespacio, pero ¿hasta dónde se logra una gobernanza digital? La cooperación interestatal y las oportunidades que generen los gobiernos para sus ciudadanos va a depender de la agilidad y flexibilidad de la introducción estatal a la Era Digital.

2.1 Contextualización

Al exponer la teoría en el contexto de la temática investigada, salen a relucir ciertas necesidades para clarificar la relación que los conceptos de estudio tienen con el tema. Es de relevancia, sintetizar la manera en que la ciberseguridad, las TIC's y la gobernanza se correlacionan para poder comprender a mayor profundidad el impacto de estos términos.

2.1.1 Tecnologías de la Información

La tecnología ha estado presente en el mundo mostrando una evolución en donde diferentes actores; personas, organizaciones y Gobiernos, las habían utilizado inicialmente para fines bélicos. En la Sociedad Internacional, con el auge del capitalismo, donde la oferta y demanda de la tecnología aumenta el crecimiento económico en los Estados inicia una transición a una infraestructura colectiva relacionada a la información determinada por el acceso a conocimiento, comunicación y desarrollo.

Es por ello, que la población hoy en día fluye en la normalidad de la tecnología, que es invisible, dinámica y siempre innovándose a sí misma. La mayoría de las personas han interactuado en algún momento con un segmento de la tecnología ya sea teléfonos, televisión, cable, radio, dispositivos móviles, computadores o Internet. Sin duda alguna, el mayor salto para las tecnologías de la información se dio en la década de 1920 con el diseño simplificado de un computador (Johnson, 2015). La introducción de cambios en el proceso de la información permite la rápida evolución de estas tecnologías hasta la actualidad, dividiéndose en varias generaciones relevantes para comprender el uso de las TIC's.

Tanto Johnson (2015) como Asensi (1993) concuerdan en la división generacional sobre la evolución de los computadores:

1. Primera Generación (1951): Fabricación del primer computador electrónico de escala industrial utilizando válvulas y dependiendo del lenguaje binario para programación.
2. Segunda Generación (1958): El transistor reemplaza las válvulas, permitiendo mayor cantidad de fabricantes para cubrir la demanda de diversas entidades.
3. Tercera Generación (1965): Computadores con circuitos integrados, se adecuan a terminales remotas comunicándose por líneas telefónicas. Se incluye programación para líneas aéreas y control de inventario en tiempo real.
4. Cuarta Generación (1971): Sustitución a los chips, con diseño del disco y diskette. Proliferación de los ordenadores personales.
5. Quinta Generación (1990): Desarrollo de los computadores inteligentes

Con una leve pincelada de la cronología referente a los computadores, cabe recalcar el progreso del Internet, que a partir de la década de 1950 consiste primordialmente en el desarrollo de tecnología de comunicación global (Padilla, 2018). De manera paralela a la tercera generación computacional, el intercambio de información se facilita y Estados Unidos comienza a liderar el proceso incremental de innovación alrededor de esta tecnología.

El contexto histórico, permite ubicar la evolución de las tecnologías de la información en un mundo polarizado, que adelanta hacia 1970 en donde se crean los protocolos NCP (Network Control Program) y TCP/IP (Internet protocol) que en resumen permiten la interconexión de programas en distintos ordenadores, conectados a diferentes redes. Esta sería la base de la infraestructura utilizada el día de hoy (Johnson, 2015). A su vez, los avances representan la opción de registrar direcciones de Internet e interconectar distintos grupos de investigación en el territorio estadounidense.

En 1989, las iniciativas alrededor de la Internet son evaluadas y financiadas para ayudar a conectar alrededor de 25 países. Mientras, Tom Berners-Lee, en el CERN, crea

la World Wide Web (WWW) utilizando hipervínculos en formato HTML para enlazar información en cualquier parte del mundo. El impacto de estos avances, han permitido que se continúen desarrollando tecnologías que han pasado de ser analógicas a digitales y han logrado convergencia entre comunicaciones, publicaciones, entretenimiento, entre otros. De esta forma los gobiernos han ido lentamente analizando los potenciales desafíos alrededor del control de los sistemas de comunicación e información.

Entonces, las Tecnologías de la Información (TIC's) de manera comprensiva según Ávila (2013) se definen:

"*Es el conjunto de herramientas, soportes y canales desarrollados y sustentados por las tecnologías (telecomunicaciones, informática, programas, computadores e internet) que permiten la adquisición, producción, almacenamiento, tratamiento, comunicación, registro y presentación de informaciones, en forma de voz, imágenes y datos, contenidos en señales de naturaleza acústica, óptica o electromagnética a fin de mejorar la calidad de vida de las personas."* p 222.

La base de la Sociedad de la Información son las TIC's, como estas se correlacionan y paralelamente, para esta investigación, como los distintos gobiernos lideran iniciativas de control, consumo, mejora y protección de los datos de la información compartida en cualquiera de los contenidos transferidos o guardados. Si bien la definición de TIC llega a ser muy amplia, ha de ser evidencia del dinamismo del mundo digitalizado y de los potenciales riesgos que los individuos, empresas y Estados corren en la transmisión continua de datos por estos canales.

Parte de las modificaciones del comportamiento individual y social que han traído las TIC's, lo exponen Muñoz y Nicaragua (2014):

1. Independencia en cuanto a la búsqueda y gestión de la información a través de la Web

2. Exigencia para menor tiempo de respuesta, que tiene un impacto en el desarrollo de velocidad de procesamiento, accesibilidad a Internet, disponibilidad de bases de datos y dispositivos para reproducción de materiales.
3. Cambio en las políticas y formas de trabajo en instituciones de servicio, puesto que genera una cantidad de transacciones elevada y servicios de forma digital (ejemplo: bancos, comercios o universidades). Esto ocasiona la digitalización de datos personales y simplificación de trámites.
4. Nuevos puntos de acceso a Internet con la masificación de acceso en la mayoría de las estructuras como hogares, trabajos y centros de enseñanza.
5. Alianzas entre los gobiernos y la empresa privada para ofrecer conectividad transformando los comportamientos de consumo.

Las TIC's deben aprovecharse para el desarrollo integral de la comunidad, sin embargo, no se puede posicionar como positivo o negativo, sencillamente porque son guiadas por el usuario y esto hará que el alcance sea definido. Si bien, se pretende por parte de los Gobiernos y otras entidades darle una orientación positiva para impulsar el progreso que impulse el potencial humano, existen peligros reales con la falta de orientación en el uso de estas. La medición continua de las TIC's en la Sociedad de la Información busca ver el alcance y las potencialidades que pueden ser mejor aprovechadas, pues se traducen a la creación de políticas públicas que contribuyan a la equidad social garantizando acceso a toda la población y disminución de la brecha digital.

Ya que las TIC's poseen características únicas que permiten el desarrollo de interacciones en todos los ámbitos de la vida, se puede clasificar como el eje principal de la sociedad del conocimiento, donde las sociedades digitales marcan el inicio de una civilización con nuevos ordenes sociales, económicos y políticos. Cabe recalcar, que el uso de las TIC's ha generado una serie de riesgos en las sociedades, como más adelante se detalla. Parte de las estrategias de utilización incluyen la inserción de las practicas sociales que deben ser medidas como herramientas potenciadoras, pero hay situaciones en donde se observa un aumento en las desigualdades, abundancia descontrolada de contenidos y fragmentación de la solidez sociológica.

2.1.2 Comunidades digitales, parte de la Sociedad de la Información

Con la aparición del Internet se han desarrollado nuevos patrones de interacción social en donde la formación de comunidades virtuales ha llegado a sustituir formas de interacción humana limitadas de manera geográfica. Los usos que se le han dado a esta forma de comunicación relacionan distintos ámbitos sociales, desde actividades familiares, trabajo y estudio hasta entretenimiento. Para entender de manera más precisa el origen de las comunidades digitales, inicialmente se debe comprender el uso del Internet en la cotidianidad.

Internet, Belloch (2015) lo define como: *"un sistema mundial de comunicaciones que permite acceder a información disponible en cualquier servidor mundial, así como interconectar y comunicar a ciudadanos alejados temporal o físicamente"*.

Es por ello por lo que gran parte del impacto de las TIC's en la modernidad, se debe a la utilización ampliada del Internet como medio para obtener interacciones de manera instantánea a cualquier lugar del mundo. El acceso de los usuarios a la adquisición de conocimientos ha sido debatido por su alcance en cuanto a calidad, proliferación y el rol activo que juega cada individuo. Belloch (2015) a su vez, señala con claridad que la información no solo construye conocimientos individuales, sino que *"puede construirlo en forma colectiva, asociándose a otros sujetos o grupos*".

La asociación de los individuos cumpliendo una serie de componentes ilustrados por Martínez, Leyva, Félix, Cecenas, & Ontiveros (2014), conforma una comunidad tradicional:

1. Un grupo de individuos con un pasado común del que se desprenden relaciones y normas de conducta con intereses comunes.
2. El grupo que forma una comunidad ocupa un territorio determinado.
3. El grupo humano que constituye una comunidad satisface necesidades básicas de alimentación, vestido, vivienda, seguridad y recreación.

4. La conversación y la reproducción de la vida humana en la comunidad se hacen en forma organizada.
5. Se advierte una separación a manera de estratos o capas.

Es por estos componentes que la comunidad conforma un tejido de relaciones sociales donde el sentido de pertenencia forma parte de la identidad del sujeto, así como la identidad común que añade cohesión posibilitando el crecimiento y desarrollo. Con mayor claridad, Moreno y Suárez (2010) indica que la comunidad es una representación social, simbólica y cultural, donde los procesos de digitalización han transformado la sociedad donde existe un espacio de flujos "*que supera a un espacio de lugares localmente fragmentado y a la estructura territorial como forma de organización cotidiana*".

Por tanto, debido al uso del Internet resalta el origen de las comunidades virtuales donde los individuos acuden con un nivel impersonal y carencia de contacto humano, es una sociedad mediática que indica un cambio de las normas sociales, por la masificación de contenidos extendidos a todas las clases sociales. Es por esto que se habla de una "cultura de masas" entendida sobre la influencia en el comportamiento humano basado en el tiempo que se pasa en línea ejerciendo cualquier tipo de actividad (Martínez, Leyva, Félix , Cecenas, & Ontiveros, 2014).

El desarrollo de la cibercultura en las comunidades digitales se extiende a relaciones contextualizadas y globalizadas de un individuo. Por lo tanto, una persona puede relacionarse con otras en contextos específicos que le provean sostenibilidad en el tiempo creando nuevas y variadas relaciones sociales alrededor de un sitio web. Sin embargo, la comunidad como tal siempre radica en el reconocimiento de la socialización, el cual se expone la interactividad de las personas por medio de la evolución de los lenguajes y las narrativas en la relación realidad y virtualidad.

La cibercultura, según Moreno y Suárez (2010) debe ser entendida como *"el conjunto de sistemas que tienen lugar en el ciberespacio, que transforma los imaginarios y discursos de los cibernautas a través de saltos e interacciones entre la interfaz y el*

mundo real (…) se desborda la virtualidad al irrumpir en la realidad de los sujetos" El impacto en la nueva interacción dicotómica con la digitalización ha permitido el desarrollo por ejemplo de la inteligencia artificial, pero al mismo tiempo ha deteriorado la creación de criterios basados en conocimiento interiorizado, e inclusive algunos autores consideran que remite a la pérdida de valores, costumbres y tradiciones aprendidas.

La representación en el espacio virtual da lugar a nuevas formas de privacidad, identidad personal y colectiva, sumada a la utilización de las comunidades virtuales que giran en torno a plataformas como YouTube, Facebook o TikTok. La necesidad de igualdad en un espacio para compartir legitima públicamente la expresión individual. Es por ello, que la línea divisoria en la dicotomía virtualidad/realidad se difumina especialmente en las generaciones más jóvenes desarrollando nuevos paradigmas que por medio de la tecnología dan representaciones culturales que el individuo normaliza. El uso del anonimato es una de estas características que permite jugar con la información presentada y moldearse a una realidad.

Al formar parte de la cotidianidad, el imaginario no es liso, sino que se acomoda a la diversidad y puede llegar a presentar variedad de comportamientos individuales de las personas que interactúan en las plataformas. Es por ello que, algunos autores, lo clasifican dentro de las *"contradicciones de la sociedad liquida, individualizada y globalizada"* (Moreno & Suárez, 2010). Las contradicciones e incertidumbre en la vida de una comunidad digital, no es fácilmente descifrada por los ciudadanos que se conectan o desconectan según las necesidades puesto que la tecnología viene a modificar y relativizar el espacio y el tiempo en las relaciones humanas.

2.1.3 Internet, la modernidad líquida y la brecha social

En el Siglo XVIII una serie de fenómenos llevaron a la caracterización de la Revolución Industrial. En la actualidad, convergen una serie de fenómenos tecnológicos que relatan la Revolución Cibercultural, entendida como *"el proceso en el que las nuevas tecnologías estas transformando las estructuras sociales, las formas relacionales y el contexto cultural(…) se trata de un nuevo entorno online en el que las relaciones sociales*

se disocian de las categorías tradicionales de tiempo y espacio" (Moreno & Suárez, 2010). Junto con la masificación de la cultura, se observa el efecto de las TIC al involucrarse para formar de la nueva existencia dejando un impacto directo en el accionar político, económico y social que debe ser ajustado a la nueva realidad.

Zygmunt Bauman es quien originalmente expone la posición liquida del entorno cibernético, entre otros, donde Moreno y Suárez (2010) interpretan que una sociedad se mueve rápidamente, simulando el estado líquido de la materia, donde las personas no tienen vínculos duraderos, sin embargo, estos son desarrollados y establecidos como modo de contacto basado en la ciberconectividad. La dialéctica entre sólidos y líquidos proviene directamente del efecto que posee Internet como poder globalizador y las situaciones específicas del individuo o comunidad.

El sistema capitalista tiene mucho que ver en la ciberconectividad, puesto que propicia el individualismo y *"marca nuestras relaciones y las torna precarias, transitorias y volátiles*" (Vásquez, 2008). La incertidumbre como parte del sistema es un peligro potencial al espacio que ocupa un individuo, puesto que se solidifica el poder invisible del sistema, aunque algunos lo califiquen como el punto de inflexión donde hay una caída de valores y el Estado pierde su peso en el imaginario como formador de opiniones frente a las tecnologías de la información, específicamente Internet, donde hay abundancia de datos que no necesariamente son necesarios, o contextualizados.

La comunicación permite a las personas interactuar en cualquier lugar mediante la tecnología, volviéndolas portátiles y apoya la desfragmentación de las comunidades tradicionales para volverlos líquidos en las comunidades digitales. Es en las comunidades, que la cibercultura se desarrolla, una vez más exponiendo la flexibilidad y la libertad de los comportamientos sociales generando un individualismo conectado (Moreno & Suárez, 2010). Donde ciertamente, el conocimiento es un valor agregado.

La demanda en la sociedad por Internet ha hecho que la integración tecnológica en ciertos países se introduzca en todo tipo de productos, de tal manera que recaen ciertos beneficios en aquellos individuos que tienen un privilegio de clase, una

jerarquización social. Se entiende en este aspecto que el mercado tiene la particularidad de generar demandas sobre diversos productos, donde el nuevo modelo es usualmente el más codiciado por las personas. Al tener una elección dentro del mercado, la sociedad está escogiendo directamente inclusividad social o la otredad (Murolo, 2010).

El punto de inflexión sobre la capacidad de liquidez en la sociedad influye la noción del otro, donde en la actualidad no todas las personas pueden alcanzar la inclusividad por medio de los diseños del mercado. Esta problemática viene en conjunto con la limitación económica para la adquisición de productos, en algunas veces de tipo básico; así como la limitación educativa especializada para acceder a la alfabetización digital. Volviéndose un impulsor de la desigualdad llamado la brecha digital que consiste según Serrano y Martínez (2003) en "*la separación que existe entre las personas (comunidades, estados, países…) que utilizan las Tecnologías de Información y Comunicación (TIC) como una parte rutinaria de su vida diaria y aquellas que no tienen acceso a las mismas y que aunque las tengan no saben cómo utilizarlas"* pero que a pesar de enfatizar el acceso a la tecnología, también se debe tomar en cuenta el acceso a la información que en el caso de Costa Rica afecta a nivel social, cultural, político y económico.

La brecha digital se puede observar en mediciones de factores tecnológicos como densidad telefónica, número de usuarios de Internet, numero de computadores, etc. Por ejemplo, en cuanto a comunicaciones inalámbricas, el América del Norte en 2016, se contaba con una cobertura de 59% y África con un 11% (Canaza, 2018). Por ello la desigualdad comunicativa representa ventajas para el desarrollo o rezago en el avance comercial, educativo, cultural, entre otros.

En Costa Rica, la brecha digital es medida bajo el Índice de Brecha Digital (IBD) cuyas mediciones constan de acceso, uso, calidad y educación en TIC's. Hallazgos en el IDB con la apertura de las telecomunicaciones indican variaciones en oportunidades de acceso, puesto que en el período 2008-2011 se dio una disminución del 27% en el IDB. También se especifica para el período una división clara entre ubicaciones geográficas para el acceso a la tecnología, la zona Norte y Atlántica Sur poseen mayor IBD que en la Región Central (Muñoz & Nicaragua, 2014).

2.1.4 Sociedad del Riesgo en la Guerra Digital

La modernidad liquida, como mencionado anteriormente, engloba la incertidumbre, la individualización en la sociedad donde se diluye el acuerdo social tornándose en fragmentos que llevan a generar miedo en un mundo capitalizado y mercantilizado, dando la búsqueda por un futuro seguro que en muchos casos se idealiza en las sociedades digitales (Canaza, 2018). El temor y la desconfianza en la realidad impulsa el imaginario de la cibercultura. Los peligros derivan también de las oportunidades generadas por el capitalismo, que lo convierten en una cuestión política.

Las amenazas sistemáticas no se concientizan dentro del debate público de manera inicial, debido a la asimetría que esto representa en el estado idealmente dual, donde la configuración social entre conexión y desconexión no representan una negatividad en la sociedad. Sin embargo, la posibilidad que los individuos enfrenten riesgos o amenazas inclusive en el mundo virtual da un sentimiento inquietante en toda la jerarquía social donde la participación se ve reemplazada por protección.

El impulso de la desvinculación personal en el proceso de individualización de las sociedades digitales sobrepone el pensamiento de Beck con respecto a las sociedades del riesgo que se vincula a la necesidad de consumo y a la brecha digital. Asimismo, el efecto de la globalización y generalización en la cultura de masas, se "*encuentran dados por medios externos al sujeto, como pueden ser el campo científico o el periodismo*" (Korstanje, 2010). Por tanto, el ciudadano comienza a perder una porción de la soberanía y los expertos de riesgo explotan la necesidad comercial de nuevos mecanismos de seguridad. "*Las irregularidades producidas por el propio capitalismo se reinventan funcionalmente en provecho del consumo masivo*" (Korstanje, 2010).

Los intereses del mercado ocasionan un efecto cíclico de necesidad, para la prolongación de los miedos y la explotación de los servicios en razón a ellos. La presentación de productos para hacerle frente a los riesgos no llega a reducir la ansiedad por lo que no presentan políticas de prevención reales. Todas las necesidades que subyacen de la sociedad del riesgo se manipulan para la producción de medios que

orientan a la protección y perpetuación de los fenómenos, pero generan una desfragmentación ocasionando una nueva estructura global que los Estados carecen de comprensión para la protección de los ciudadanos. La falta de conectividad deriva en una idea de agresión.

Las definiciones arquetípicas de la sociedad, como independencia, libertad y lo militar se han transformado de forma que se dilucida una nueva conceptualización de ellas. Se ha definido de prioridad, en el concepto de las TIC's y las sociedades digitales como la libertad e independencia llegaron ahondar características novedosas. Lo militar, que deviene de la protección de los Estados para con sus habitantes, también ha evolucionado en lo que Cundins (2017) tipifica como la desregulación de la disputa armada que debido a una simplificación intelectual cambio la percepción de los instrumentos destinados a solventar los problemas internacionales donde la sociedad liquida torna insignificantes la visión histórica y educativa de lo aprendido del mundo bélico.

La guerra en el mundo democrático se convirtió en un tema político, donde sin apoyo popular, un respaldo consensuado, no se puede ganar. Sin embargo, la infinita cantidad de amenazas que acechan a una nación, por un conflicto entre la seguridad interna y externa; explotan la ineficiencia estatal de reacción. La desconfianza ocasiona una revisión de capacidades que pretenden un funcionamiento en un mundo distinto para lo que fueron creados, desde el narcotráfico, el terrorismo y los ciberataques renuevan los actores de los conflictos; que son distintos a los Estados.

Por tanto, el final de la guerra era la continuación de la política, o del acuerdo político. Este sector del conflicto hace que la sociedad surja como un verdadero actor y que las asimetrías de los actores hicieran de las estrategias y procedimientos algo diferente, calificándola como guerra hibrida. Esta comprende que "*uno de los bandos en notable inferioridad de condiciones materiales que el otro, utiliza no solo acciones convencionales y no convencionales, sino también acciones de guerrilla, de terrorismo y de crimen organizado"* (Locatelli, 2017). Además, que "*más allá de la violencia física, estos acontecimientos pueden expresarse en varios planos simultáneos, entre ellos el*

económico, legal, cibernético, comunicacional y mediático" (Bartolomé, 2019). Queda claro que clasificar un conflicto híbrido va más allá de una situación bélica tradicional, sino que enfrente actores no tradicionales como hackers en planos que los Estados no tomaban en cuenta como el ciberespacio.

La asimetría, asincronía y el uso de las TIC's otorga gran importancia al manejo psicológico y masivo de los medios de comunicación, donde desde la Guerra de Iraq con la Operación Tormenta del Desierto se visualiza una guerra de inteligencia, electrónica y contra inteligencia. Fue a partir del 9/11 que hubo una actualización teórica donde se ratifica el uso de los medios y las redes informáticas para distribución de mensajes en una sociedad fragmentada -líquida. El carácter multidimensional hace que el proceso de comunicación no dependa del tiempo o espacio, siendo la cooperación, control y desarrollo de la cultura de seguridad las bases para el uso inteligente e intensivo de los sistemas de información y conocimiento.

La guerra digital o guerra de la información consiste en "*el desarrollo de programas de control tecnológico y percepción informacional que busca multiplicar el poder militar y la capacidad de movimiento en conflictos bélicos, ampliando los horizontes cognitivos de las fuerzas militares convencionales*" (Sierra, 2003) Además se configura en distintas áreas como seguridad operacional, guerra electrónica, operaciones psicológicas, engaño, ataque a procesos de información. Esta última se remite al uso de TIC's para apagar virtualmente, degradar, corromper o destruir los sistemas de información de un enemigo.

Basándose en lo anterior, los medios de información y la estrategia militar convergen en una cultura mediática de videovigilancia global, siendo la seguridad un principio en la vida pública que es una "*nueva disciplina de regulación y acomodamiento social de la conciencia cívica a las necesidades de orden y control político-militar por razones preventivas*" (Sierra, 2003).

La guerra digital ha llegado a expandir la forma en que el control de las tecnologías por parte de los actores de la Sociedad de la Información logra consolidarlos y hace

referencia a la necesidad de regulación social en todos los ámbitos. Los individuos de forma directa o indirecta son vigilados, y llevados a un proceso cognitivo de estrategias pensadas para mantenimiento del orden dentro de una libertad fragmentada.

En el caso de la seguridad nacional estadounidense cabe recalcar que el espacio radioeléctrico es definido por Sierra (2003) como "*un área estratégica de interés nacional para la concepción comunicativa del ejército, imbricando de este modo en la responsabilidad del control y la política de seguridad de las redes satelitales al propio sector privado*". Es por ello que la mayoría de las estrategias de Seguridad Nacional se crean con base en este tipo de situaciones para planificar y desarrollar TIC's con fines militares puesto que la guerra de la información es sobre la influencia sobre la sociedad y las decisiones que se toman.

La pérdida de protagonismo de los Estados en la seguridad nacional hace que actores no estatales como las empresas privadas tengan también una influencia en la toma de decisiones frente a riesgos y amenazas al crear Estrategias de Seguridad Nacional. Estas corresponden directamente a las necesidades y trata de integrar todos los instrumentos para hacerle frente a los peligros. Mientras que países como Estados Unidos o España han modificado su visión defensiva, en Latinoamérica de forma generalizada la sociedad no se determina como blanco del terrorismo. Es por esta razón y la historia latinoamericana con respecto a las dictaduras, que seguridad nacional se vislumbra como mantenimiento del orden.

Por otro lado, en el ciberespacio, se ha esbozado también tanto la guerra de la información como la guerra hibrida. La ciberguerra tiene diversos componentes novedosos expuestos por Bartolomé (2019):

1. El ciberespacio es el dominio global compuesto por infraestructuras de TIC.
2. Actuación en red tanto de forma de actuar como de organización.
3. Incorporación de actores de diferente tipo.
4. Priorización de la infraestructura critica (sistemas, máquinas, edificios o instalaciones relacionados con la prestación de servicios esenciales)

2.2 Perspectivas de la Ciberseguridad

En la actualidad, existe un déficit entre la realidad y las necesidades sobre la seguridad en el ciberespacio debido al desarrollo de las garantías sobre la identidad de las personas y las organizaciones. La digitalización de la economía y la masificación de las TIC's ha generado riesgos y amenazas para la ciudadanía que requiere por ejemplo de la utilización de contraseñas para existir en el ciberespacio.

El entendido sobre el ciberespacio radica en una zona construida que permite considerar procesos dentro de una red de valores y normas que desarrollan comportamientos donde el mismo se vuelve soberano. Son los poderes estatales externos quienes intentan asegurar la regulación de los espacios. Por tanto, la agenda de los Estados con respecto a la ciberseguridad conforma un reto debido a la discrepancia entre la reacción de un gobierno con la evolución del ciberespacio.

Este último es aquel que entrecruza la realidad y lo virtual, donde interpone lo militar, lo vivencial y lo tecnológico en la sociedad. En el caso costarricense, la navegación en el ciberespacio depende primariamente del uso de dispositivos móviles. Con el manejo de plataformas y aplicaciones digitales, los individuos dejan marcas digitales o huellas en donde existen interconexiones que relacionan la identidad física personal con la virtual y esto tiene implicaciones con el manejo de los datos en el ciberespacio. Quirós-Ramírez (2019) aclara que la posibilidad de exposición a amenazas y riesgos con las nuevas formas de registro de la identidad personal-virtual se potencia. En las sociedades digitales, la huella digital es parte de la Nube Virtual (Cloud) que hace posible el análisis de comportamientos o segmentación de perfiles haciéndolo relevante con fines de seguridad digital.

Los riesgos que se asocian a la digitalización dependen de 3 factores descritos por Fischer (2016):

1. Amenazas: Personas o grupos que realizan ciberataques; son considerados: otros Estados, organizaciones criminales, ciberterroristas, ciberactivistas, organizaciones privadas, agentes internos.

2. Vulnerabilidades: La ciberseguridad depende ampliamente de una carrera entre atacantes y defensas. La infraestructura usualmente compleja, pero existen atacantes que se encuentran constantemente en la búsqueda de debilidades. Hay varios tipos de vulnerabilidades inmensamente desafiantes como actos inadvertidos o intencionales por partes de personas con acceso a un sistema; vulnerabilidades de la cadena de suministro y vulnerabilidades previamente desconocidas (zero day) sin solución establecida. En algunos casos, se dificulta el manejo de vulnerabilidades por manejos presupuestarios u operativos.
3. Impacto: Cuando un ataque llega a comprometer la confidencialidad, integridad y disponibilidad de la infraestructura o la información que se maneja. En estos casos, el efecto sobre la seguridad nacional, economía, seguridad de los individuos tiende a ser parte de la forma de trabajo.

La sociedad, los grupos y las instituciones tienen distintos grados de vulnerabilidad, así como oportunidades de defensa. La implementación de las medidas de protección depende, según sea el caso de los individuos, las instituciones, entidades legales y gubernamentales. Entonces, la ciberseguridad dentro de la esfera costarricense es concebida como *"la disminución del riesgo y la neutralización de las amenazas integran el concepto de seguridad dentro del mundo virtual*" (Quirós-Ramírez, 2019). Mas allá de esta conceptualización, el acto de protección de la infraestructura crítica y su contenido, indica Fischer (2016) que debe referirse a:

1. Un conjunto de actividades y otras medidas destinadas a proteger contra ataques, interrupción u otras amenazas: computadoras, redes de computadoras, hardware relacionado y software de dispositivos y la información que contienen y comunican incluyendo software y datos, así como otros elementos del ciberespacio.
2. El estado o la calidad de estar protegido de tales amenazas.
3. El amplio campo de esfuerzo dirigido a implementar y mejorar esos actividades y calidad.

Se puede generar cierta confusión al respecto, puesto que la ciberseguridad engloba la protección de medio digital pero la información puede ser observada por el

ciudadano como privada. Entonces, la ciberseguridad podría llegar a determinar un medio de defensa frente a vigilancia indeseada, así como la recopilación de información en un sistema. Pero que, a su vez, cuando se trata de ciberataques estas mismas actividades puede ser útiles para la ofensiva y el monitoreo del flujo de la información en el sistema.

Un ciberataque es clasificado como "*un intento no autorizado por la vía digital de acceder a un sistema de control, dispositivo electrónico y/o red informática, con el propósito de sabotear su funcionamiento, extraer información y recursos, o extorsionar a usuarios y organizaciones*" (COMEXI, 2018). En síntesis, la defensa o protección de actividades consideradas maliciosas y no autorizadas por medio de las TIC's posee valor directo con la sociedad y el Estado, especialmente debido a la vulnerabilidad psicológica que estos tipos de ciberataques pueden tener en un país.

Para los gobiernos la dificultad alrededor de la creación de políticas se debe al incremento de las amenazas. Los ataques a entidades públicas y privadas han incrementado un 61% (OAS, 2013). De igual forma, la implementación de CSIRTs ha permitido la detección y mejor vigilancia sobre actividades cibernéticas ilícitas. En general, las principales amenazas en América Latina se dirigen a ataques por malware para robo de datos sensibles o confidenciales y técnicas como phishing (correo electrónico que infecta un computador) y watering-hole (infiltración de sitios web para mandar códigos maliciosos) (OAS, 2013). Las tendencias regionales y globales presentan similitudes en cuanto a las motivaciones de los ciberataques, donde el sector privado y sus usuarios corren mayores riesgos de ataque que aquellos vinculadas a ataques a entidades públicas.

La clasificación internacional sobre los tipos de ataque se cataloga de acuerdo con Pérez (2019) en:

1. Malware: Aquel software destinado a realizar un proceso no autorizado que tendrá un impacto adverso en la confidencialidad, integridad o disponibilidad

de un sistema de información. Se subdivide en: virus, spyware, adware, rootkit, troyanos, worm, ransomware, keylogger, botnet.

2. Phishing: Técnica para intentar adquirir datos confidenciales, como números de cuentas bancarias, a través de una solicitud fraudulenta en un correo electrónico o en un sitio web.
3. MitM (Man in the middle attack): Cuando un atacante altera la comunicación entre dos usuarios, haciéndose pasar por ambas víctimas para manipularlos y obtener acceso a sus datos.
4. DDoS (Distributed denial of service attack): Un ataque de denegación de servicio inunda sistemas, servidores o redes con tráfico para agotar los recursos y el ancho de banda. Como resultado, el sistema no puede cumplir con solicitudes legítimas. Los atacantes también pueden usar múltiples dispositivos comprometidos para lanzar este ataque.
5. SQL injection: Se inserta código malicioso en un servidor que utiliza SQL. Sólo tienen éxito cuando existe una vulnerabilidad de seguridad en el software de una aplicación dando acceso o para modificar datos.
6. Zero day attack: Un ataque que explota una vulnerabilidad de hardware, o software desconocida anteriormente. Puede ocurrir cuando una vulnerabilidad se hace pública antes de que el desarrollador haya implementado un parche o una solución.

Los delitos informáticos tienden a ser parte de un amplio espectro de actividades como bienes y servicios ilegales; piratería informática; prostitución; robo; hurto de la identidad; entre otros. Todos estos relacionados de una u otra manera a los instrumentos para cometer estas infracciones: los computadores y el Internet. El auge de la tecnología incrementa la tendencia de los delitos. Otra categorización sobre los ataques según COMEXI (2018) es de ataques dirigidos y no dirigidos, donde depende de la meta ya sea vulnerar un individuo o grupo o una meta más general como se expone en el cuadro 1.

Cuadro 1. Tipos de ataques: Dirigido y No Dirigido

Ataque Dirigido: Tipo de ataque en el que se vulnera la infraestructura, sistema o procesos de una entidad especifica			
Ataque no Dirigido: La forma más común y generalizada de lanzar un ciberataque, enfocada a causar daño a la infraestructura o sistemas de un grupo de individuos o empresas de forma indiscriminada			
Tipo	Ejemplos de Técnicas	Descripción del ataque	Ejemplos de ataque
Dirigido	Spears-Phishing	Enviar correos electrónicos a individuos específicos que contengan un archivo adjunto con software malicioso	2015: Un Ataque a la oficina de Administración Personal de los EE. UU, llevo al robo de la información de más de 21.5 millones de personas
	Zero Day	Explotar vulnerabilidades no conocidas públicamente a sistemas de empresas especificas	2012: Un ataque a Saudi Aramco que destruyo 35000 computadoras en unas cuantas horas
	Subversión de cadena de suministro	Atacar a un equipo o software antes de que sea entregado a una organización	El adware Superfish, preinstalado en las notebooks Lenovo permitió a los atacantes hacerse pasar por diversas direcciones de internet
No Dirigido	Phishing	Enviar correos electrónicos a un gran número de individuos pidiendo información sensible o alentándolos a entrar a una página con código malicioso	2016: Shamon 2 afecto a más de 15 instituciones privadas y agencias de gobierno en Arabia Saudita
	Ransomware	Diseminar Malware enfocado a extorsionar a empresas e individuos (p. ej. malware que puede negar el acceso del usuario a su computadora a menos que se pague un rescate)	2017: El incidente WannaCry que afecto a más de 300000 equipos y comprometió la seguridad de empresas en más de 150 países
	DDoS	Utilizar código malicioso para dirigir a computadoras infectadas a abrumar un sitio o servicio en la red, afectando su funcionamiento	2016: El ciberataque Dyn afecto la disponibilidad de múltiples plataformas y servicios en internet
	Campañas de desinformación	Utilizar bots, sitios que emulan medios legítimos, redes sociales y otras herramientas para manipular la opinión pública o influir sobre la toma de decisiones de grupos.	2017: Esfuerzos para manipular los resultados de la elección francesa (hackeo el partido En Marche!. publicación de mails incluyendo correos falsos, etc.)

Fuente: COMEXI (2018)

La variedad de ataques cibernéticos da una idea de la rapidez con que evoluciona el ciberespacio y las dificultades que tienen los especialistas para encontrar las amenazas y vulnerabilidades en el sistema. Con cada mejora, cambio de proceso o innovación de dispositivos los cibercriminales se encuentran dispuestos a presentar la variación a las reglas con las que él se rigen las empresas e instituciones. Las herramientas no solamente funcionan para encontrar datos en las plataformas, sino también como una forma de movilizar a la población frente a un tema de opinión pública. La fragilidad del uso de las TIC se evidencia de esta manera y la responsabilidad de todos los actores con algún poder del ciberespacio queda plasmada en la formulación y operalizacion del manejo de esta virtualidad. Los Estados, las empresas privadas y las comunidades digitales se enfrentan a un cambio en el paradigma de la información en la Sociedad del Riesgo y la educación y sensibilización alrededor de la utilización de los datos deja un precedente significativo en la formulación de políticas públicas.

2.2.1 Estrategia y evolución de la ciberseguridad en Estados Unidos

La necesidad de obtener información ha transformado la operación sobre el manejo, control y protección de datos. Las actividades cibernéticas maliciosas por parte de varios Estados presentan un acelerado crecimiento. Los individuos que llevan a cabo el ciber espionaje, son altamente calificados, haciendo que el trabajo de prevención o defensa sea más complejo. Muchos Estados han sido parte, históricamente, de estrategias para obtener información de esta manera.

Mas allá de lo anterior, en varias ocasiones y como parte de la estrategia de seguridad, Estados Unidos ha llegado a identificar código malicioso y técnicas de ataque que atribuyen distintos ciberataques por parte de Rusia, China, Irán y Corea del Norte. Es común que China sea catalogado como principal actor estatal que contribuya al hackeo, por ejemplo, el Pentágono ha reportado al Congreso estadounidense sobre actividades en detrimento de la ciberseguridad del sector público y privado del país (The Council of Economic Advisers, 2018).

A nivel interno, Estados Unidos ha tratado de armonizar los esfuerzos para contrarrestar los riesgos asociados a la ciberseguridad. A partir de 1990, con un decreto presidencial se establece una estructura cuya finalidad es coordinar las actividades entre el sector público y privado para eliminar cualquier vulnerabilidad significativa de las infraestructuras críticas. Este decreto se actualizo en el 2003, transformándose en la Estrategia Nacional de un Ciberespacio Seguro. En conjunto con la Secretaria de Seguridad Nacional trabajan para coordinar los esfuerzos de protección de esta infraestructura.

En el 2007, la Iniciativa Nacional de Ciberseguridad (CNCI) cambio su estrategia unificándola de defensiva a cohesiva con la legislación, inteligencia y capacidades militares para abordar amenazas cibernéticas como intrusión de redes remota, operaciones internas y cadena de suministro de vulnerabilidades. Adicionalmente en *Cyberspace Policy Review* (2009) se detallan puntos que continuaran siendo vigentes en la Estrategia Nacional de Ciberseguridad: liderazgo desde la Casa Blanca, capacitando a la nación digital, compartiendo responsabilidades para la ciberseguridad.

El sector privado muy a menudo depende del gobierno para evitar ataques cibernéticos sin embargo las empresas tecnológicas como Google, Microsoft, Apple y Verizon poseen información que han tenido que coordinar para el desarrollo de políticas públicas actualizadas e interiorizarlas al uso de la sociedad estadounidense. El conocimiento acerca de la naturaleza de los ciberataques demuestra que no existe, en la actualidad, un manual de tácticas, pero con cada ataque se revelan datos sobre la ingeniería y las capacidades de los actores. Esta es la base para el mapeo en la coyuntura actual, información que tanto el gobierno como el sector privado analiza junto con expertos.

Una de las razones principales por la que se depende del análisis del gobierno, se debe directamente a falta de detección; falta de protección e infraestructura, por parte del sector privado. Se ha indicado que cerca del 71% de vulnerabilidades no son detectadas (The Council of Economic Advisers, 2018) y que las instituciones gubernamentales observan comúnmente violaciones a la seguridad de las empresas.

Por ejemplo, el Centro de Estudios Estratégicos Internacionales informa que se notificaron en 2013, unas 3 000 empresas que habían sido pirateadas. Las razones por las que no se informan los ataques, tiene que ver con el valor del mercado de las mismas. Es posible que, si un ataque es masivo, a unas 34 empresas, únicamente 1 reporte dicho ataque.

Estados Unidos ha definido que los sistemas y activos de la infraestructura critica tienen un impacto directo en la seguridad nacional, la seguridad económica nacional, y la seguridad nacional publica, por lo tanto, incapacitarle o destruir estos sistemas significaría un debilitamiento generalizado para el Estado. Algunos de los sectores de mayor relevancia para la ciberseguridad y la economía americana son: energía, aeroespacial y defensa, tecnología y telecomunicaciones (The Council of Economic Advisers, 2018).

El costo de las actividades maliciosas cibernéticas es desconocido debido a la falta de reportes, de detección o falta de cuantificación del impacto; la huella asociada a los efectos indirectos para las empresas, aumento en presupuesto y gasto en ciberseguridad, contención al impulso económico debido a la amenaza cibernética se podría observar como un detrimento para el crecimiento económico americano. Sin embargo, el sector se encuentra en crecimiento y la innovación tecnológica es de suma importancia para la estrategia del país. El efecto en cascada en este caso implica potencial de exportación de tecnología y servicios que genere desarrollo de programas educativos para el sector.

2.2.2. Ciberseguridad en América Latina: México y Costa Rica

Generalmente, las estrategias de ciberseguridad en los países desarrollados son consideradas integrales pues abarcan desde aspectos económicos, educativos, jurídicos, militares y relacionados con la inteligencia. Cuando estas estrategias se centran en asuntos militares se da un desequilibrio en la propuesta dejando de lado ciertos derechos humanos como privacidad, libertad de expresión y asociación. Por tal razón, la relevancia de crear estrategias en América Latina y el Caribe está en aumento,

pero el nivel de madurez de los Estados varía desde el marco para cooperación hasta la distribución interna.

En la región, la coordinación en el desarrollo de la política de seguridad cibernética no ha sido llevada a cabo por el ejército y las entidades de seguridad nacional. Esto podría considerarse un equilibrio, mas es una oportunidad para el desarrollo de políticas públicas de ciberseguridad en donde diversos actores de la sociedad sean incluidos. Los países de la región se encuentran con la opción de renovar la percepción de la ciberseguridad que no se deriva únicamente de los dominios militares y de defensa, sino que más bien se concentra en la visión humanista, en los derechos humanos.

La cooperación, aunque es relativamente restringida, se observa en la iniciativa de los Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT) que están en toda la región. Esto permite la generación de prácticas adecuadas para el intercambio de conocimientos, dando paso a la creación de sistemas de comunicación más seguros y mejorando la confianza en los servicios digitales públicos y privados que es la base de una gobernanza electrónica integral.

Preocupaciones regionales alrededor de la ciberseguridad son: la creación o modificación de legislación que defina y penalice con claridad los delitos cibernéticos y la protección de la privacidad y los datos en línea. Resulta llamativo que ambas tengan cierta legislación en Costa Rica y México pero que según el Observatorio de la Ciberseguridad en América Latina y el Caribe (2016) "*la retención de los datos obligatorios es una práctica cada vez más utilizada en la región y, en muchos casos, se pueden obtener datos almacenados sin una orden judicial*". Lo que deja abierta la recolección de datos a iniciativas públicas que no sean aclaradas debidamente a la ciudadanía reduciendo las reglas sobre la privacidad y limitando los derechos fundamentales de los usuarios de Internet.

En México, la penetración de Internet ha ido elevándose, mientras que en 2016 se calculaba que el 57% de la población tenía acceso para el 2019, esta ha aumentado a 60% (Aguilar-Antonio, 2019). La población con mayor uso del servicio se encuentra

entre los 18 y los 34 años y ellos utilizan los dispositivos para acceso a redes sociales. Los cambios a nivel social sobre el uso de dispositivos y tecnología se ven afectados por la lenta conexión, elevado costo, falta de educación y problemas con los proveedores de Internet. Por otro lado, aquellos individuos con mayor nivel de escolaridad tienen mejor acceso a actividades que involucran el uso del Internet (94% de los universitarios contrario a 46% con educación primaria) (Parraguez Kobek, 2017).

Es el país, después de Brasil, con el mayor número de ataques cibernéticos en la región y se estima que el costo de los delitos de estos ataques fue de alrededor de 3 billones de dólares. La Unión Internacional de Telecomunicaciones (ITU) ha identificado los CSIRT en la región, ubicando a México en el puesto 18 de 29 en preparación para potenciales ciberataques (Parraguez Kobek, 2017). Se debe recalcar que la entidad que maneja la cooperación con la comunidad internacional es el CERT-MX creado en 2010 y la Policía Federal es la responsable por investigar los ciberdelitos a nivel nacional.

La Estrategia Nacional de Ciberseguridad en México fue coordinada por diversas instituciones, entre ellas la División de Policía Científica de la Policía Federal, quienes recibieron alrededor de 51 000 denuncias ciudadanas, desactivaron 17 000 sitios fraudulentos y emitieron más de 2 000 alertas de ciberseguridad en 2017 (Aguilar-Antonio, 2019). En términos generales, debido a la normativa, el impulso económico y social que se le da al tema de seguridad cibernética, México es considerado con capacidades intermedias en términos de protección e investigación de casos.

Según reporta Quirós-Ramírez (2019) datos de la Escuela de Estadística de la Universidad de Costa Rica indican que el 67% de la población tiene acceso a Internet y se utiliza principalmente para visitar redes sociales (76%), para estudiar o trabajar (74%) y otras actividades como transacciones bancarias o compras en línea. De igual manera, la población que utiliza Internet ha sido: acosada (25%), experimentado algún tipo de estafa (13%) o enfrentado problemas por algo que fue publicado.

En general Costa Rica, es un país que se considera una zona tibia o intermedia en términos de ciberataques. En 2016, se ocupa el séptimo puesto en ataques

cibernéticos en la región. A partir de este año, ha tenido incrementos progresivos en el número de causas activas en la Fiscalía, mientras que en 2006 fueron alrededor de 1000 casos, entre 2008 y 2011 solo se reportaron 300 causas anuales (Quirós-Ramírez, 2019). Esto ha llegado a ocasionar interrogantes sobre el manejo de los delitos cibernéticos en a nivel interno pues a pesar de estos reportes, se han dado casos en entidades gubernamentales como la Caja Costarricense del Seguro Social, que se han visto vulnerados y el país ha estado expuesto a críticas internacionales por sabotaje informático tras el caso de los Panamá Papers.

En cuanto a comunidades virtuales, en donde la apropiación de espacios y actividades es vital, existe una población vulnerable: los adolescentes. Por definición, en esta población destaca el potencial del Internet como herramienta para promover el desarrollo de un país, y también para que sean propensos a recibir algún tipo de ataque. Es por ello que fomentar buenas prácticas sobre ciberseguridad en el marco de educación y gobernanza se vuelve crucial. Por otro lado, otros datos relevantes para la penetración de las TIC's y su protección contra ataques cibernéticos indica que la tenencia de tecnología entre las áreas urbanas y rurales es del doble (Muñoz & Nicaragua, 2014); relacionando directamente la captación de ataques en zonas urbanas.

El Ministerio de Ciencia y Tecnología (MICITT) es la autoridad principal responsable del manejo de la situación y el desarrollo de políticas relacionadas a la ciberseguridad. Hay también otras instituciones que trabajan en conjunto con el MICITT como la Secretaría Digital, la Sección de Delitos Informáticos del Poder Judicial y la Agencia de Protección de Datos de los Habitantes, entre otros. En el 2012, se establece la creación del CSIRT-CR que coordina las funciones de organización y control de la seguridad cibernética nacional, así como enlace de cooperación internacional. El hecho que el país no cuente con ejército ha suscitado en una evaluación del potencial de resiliencia cibernética nacional.

Según el Observatorio de la Ciberseguridad en América Latina y el Caribe (2016) *"la sensibilización pública de la seguridad cibernética es generalmente baja y la sociedad toma pocas medidas para protegerse de las amenazas cibernéticas".* Evidencia de lo

anterior se posiciona en la cantidad de denuncias que suscitaron a partir del 2013, junto con la penetración en auge de los dispositivos móviles y los riesgos que acarrean.

La necesidad evidente de desarrollar soluciones para los riesgos y vulnerabilidades digitales ha llevado a Costa Rica a la creación de una Estrategia Nacional de Ciberseguridad. Tanto para la atención de ataques, como para aumentar el desarrollo de la sociedad, la resiliencia cibernética y la cooperación nacional e internacional. Para la construcción de la estrategia nacional, presentada en 2017, se toma en cuenta la experiencia técnica de la Organización de los Estados Americanos y los principios rectores:

1. Las personas son la prioridad.
2. Respeto a los Derechos Humanos y la Privacidad.
3. Coordinación y corresponsabilidad de múltiples partes interesadas.
4. Cooperación Internacional.

Las TIC's al ser un catalizador de desarrollo permiten que la sociedad se interconecte, y la Estrategia Nacional (2017) pretende centrarse en las personas que utilizan de la tecnología con la responsabilidad compartida del uso de dispositivos y redes con el Estado. Es por esta razón, que la ciberseguridad se torna en un tema educativo y cultural pivote de los comportamientos sociales costarricenses. Lograr que un ciudadano promedio reconozca la importancia de la ciberseguridad en su vida cotidiana, así como la relevancia para la protección de datos y el rol que juega el Gobierno en la toma de las decisiones alrededor del cibercrimen es nuestro nuevo paradigma como sociedad.

2.2.3 La legitimidad y la legislación en Costa Rica

La sociedad cuenta con elementos que le caracterizan como tal: una población, un territorio, pero además necesitan de reglas de organización y el método para el cumplimiento de estas. El desarrollo de estas características converge en el Estado como forma consolidada de ejercer el poder político. Un artefacto social para dirigir y controlar las comunidades políticas que plantea el mantenimiento y en la mayoría de las ocasiones, el incremento del poder por parte de los gobernantes. Históricamente, el uso

de las armas ha sido esencial para lo anterior planteado, sin embargo, la asociación de las leyes justifica la "*posesión y uso del poder a través de una construcción ideológica que infunda en las mentes de los súbditos la creencia en el derecho del gobernante a mandar*" (López, 2009). Básicamente, la legitimidad y la legitimación provienen de la garantía del uso de un poder frente a una sociedad, donde la sociedad permite este ejercicio de mandar.

Entonces, la legitimidad es concebida como un reconocimiento de poder externo e interno, los gobernantes son los titulares del poder y tienen derecho de "*crear y aplicar normas jurídicas, disponiendo del monopolio de la fuerza, de acuerdo con esas normas, sobre la población*" (López, 2009). La legitimidad se encuentra más allá de una construcción jurídica, pues implica un núcleo moral que contiene derechos humanos. En Costa Rica, la legitimidad del sistema es un pilar para la estabilidad democrática.

El entorno para la legitimidad y gestión del ordenamiento se vuelve una tarea compleja entre una variedad de sujetos y relaciones, públicos y privado, civiles y organismos internacionales, etc.; y la seguridad cibernética tiene un papel central en el contexto de un Estado de Derecho. La legitimidad en el ciberespacio modifica el concepto donde el un ciudadano manifiesta su individualización y pone en ejercicio sus derechos humanos en un medio artificial que no está bajo la soberanía directa de un Estado.

En Costa Rica, la legitimidad por medio de la ley en cuanto a ciberseguridad inicia con la regulación de los delitos informáticos a partir de 1995 con el Código de Normas y Procedimientos Tributarios (artículos 93 al 97) y la Ley General de Aduanas (artículos 221 y 222). Posteriormente, la protección de los derechos de autor, correspondiente a la Ley de observancia de los derechos de propiedad intelectual en el 2000 induce a un mejor enfoque sobre seguridad cibernética (PROSIC, 2010).

En el 2001, la promulgación de la Ley de Administración Financiera y de Presupuestos Públicos incluye un artículo relacionado con la ciber delitos, pero es con la introducción en el Código Penal, de violaciones de comunicaciones electrónicas, fraude informático y alteración y sabotaje informático que realmente se da una innovación

jurídica regional. En el 2012-2013 se da una reforma al Código Penal en cuanto a los Delitos Informáticos tipificando con mayor claridad la materia favoreciendo el abordaje de los casos en Costa Rica frente al daño informático, el daño agravado, el sabotaje informático y añade la suplantación informática, el espionaje informático, la instalación o propagación de programas informáticos maliciosos, la suplantación de páginas electrónicas, la facilitación del delito informático y la difusión de información falsa (Quirós-Ramírez, 2019). Esta legislación se considera como más específica y con mejoras en la interpretación de la Ley, facilitando el potencial para alianzas internacionales que combaten el crimen cibernético.

En la Estrategia Nacional de Ciberseguridad (2017) se toma como marco regulatorio la siguiente legislación:

1. Ley General de Telecomunicaciones y la Ley de Fortalecimiento y Modernización de las Entidades Públicas del Sector Telecomunicaciones, complementado con el Reglamento sobre Medidas de Protección de la Privacidad de las Comunicaciones y el Reglamento del Usuario Final de los Servicios de Telecomunicaciones: en conjunto se trabaja protección del usuario mediante medidas como la integración de bases de datos de terminales robados/.
2. Ley de Protección a la Niñez y la Adolescencia frente al Contenido Nocivo de Internet y Otros Medios Electrónicos.
3. Ley de Protección de la Persona frente al tratamiento de sus Datos Personales y su Reglamento.
4. Ley de Delitos Informáticos y la Reforma de varios artículos y modificación de la sección VIII, denominada Delitos Informáticos y Conexos, del título VII del Código Penal: constituye un marco jurídico penal acorde a los nuevos delitos cometidos por medios tecnológicos.
5. Decreto Ejecutivo N° 40546-RREE: Adhesión a la Convención sobre el Cibercrimen, Convenio de Budapest.

Considerando la necesidad existente para el desarrollo de la estrategia nacional, es inherente la utilización de un marco robusto que dé cabida al desarrollo de distintos

sectores del Estado y la colaboración potencial con la empresa privada y otras entidades interestatales. A sí mismo, el marco jurídico costarricense añade una contextualización mayor a los usos de las tecnologías de la información y posteriormente la manera de manejar y proteger las derivaciones de esta.

Otras acciones y avances jurídicos en el marco del uso de la información contenida en medios informáticos o redes sociales corresponden según Quirós-Ramírez (2019):

1. Constitución Política: indica la protección de datos personales de los habitantes, derecho a la libertad y del secreto de las comunicaciones.
2. Código Civil: indica el derecho a la imagen.
3. Código Comercio: alude al secreto bancario.
4. La Sala Constitucional tiene el recurso de Habeas Data, donde establece las bases jurídicas para la protección informativa.
5. Ley de Protección de la Persona contra el Tratamiento de sus Datos Personales que se crea con el objetivo de garantizarle a cualquier persona el respeto a sus derechos fundamentales de autodeterminación personal, específicamente en el principio de Autodeterminación Informativa que garantiza la defensa del tratamiento de su información personal.

2.2.4 La gobernabilidad y la gobernanza en la Sociedad Digital

La gobernabilidad planteada por Camou (2001) es comprendida como "*un estado de equilibrio dinámico entre el nivel de las demandas societales y la capacidad del sistema político (estado/gobierno) para responderlas de manera legítima y eficaz*". Esta concepción del término indica que hay algunos factores que se perfilan en un nivel de gobernabilidad tomando en cuenta la importancia de la cultura política, el Estado y las políticas públicas consideradas estratégicas para el rendimiento eficaz del mismo. En Latinoamérica, históricamente se ha caracterizado por la atención a este tema puesto que la cuestión del Estado resultaba más relevante en el contexto que el ejercicio del

gobierno, como este se construye, se desarrolla la toma de decisiones y se evalúa el impacto de estas. Básicamente, el desarrollo de la gobernanza.

La aparición del término de gobernanza esté ligado al efecto de la globalización, los avances tecnológicos, auge de los organismos no gubernamentales y el papel que juega la sociedad civil en la política enfrentando la crisis del modelo tradicional del Estado. El efecto del liberalismo económico hace que las estructuras deban adaptarse a un marco cuyo objetivo es reorganizar la responsabilidad dentro de la sociedad, definiendo una evolución y variación de la gobernabilidad hacia la gobernanza.

En 1994, PNUD define la gobernanza en Initiatives for Change:

"*la gobernanza puede ser considerada como el ejercicio de la autoridad económica, política y administrativa con el objetivo de manejar las cosas de un país en todos los niveles. Ella engloba los mecanismos, procesos e instituciones por las cuales los ciudadanos y los grupos expresan sus intereses, ejercen sus derechos jurídicos asumiendo sus obligaciones*" (Documento del PNUD, 1994, citado por Le Texier, 2004).

La transición conceptual implica cierta crisis del Estado y su reformulación con la sociedad globalizada. Lo político del Estado deriva en una fragmentación hacia la nueva concepción del mundo, la dinamización económica y social. Una homogenización cultural que junto con el capitalismo y su ideología en la sociedad civil conlleva a una reivindicación de los derechos humanos, las regulaciones sociales y un equilibrio entre los actores. El debilitamiento del Estado, en su forma tradicional, permite que otros espacios para el desarrollo social sean más evidentes y que las políticas estatales aseguren el bienestar en todos los ámbitos. Sobre el desarrollo de los espacios es que se encuentra la sociedad digital, que permite producir nuevas reglas del juego permitiendo el dialogo y la acción colectiva.

La digitalización ha llevado a los Estados a la adopción de tecnologías, las diferentes iniciativas de gobierno digital ejemplifican este fenómeno. Al migrar los servicios públicos a medios digitales, donde la información recopilada incluye estrategias,

datos personales, etc., se genera una infraestructura critica para cada país. La construcción de políticas públicas de la mano con la tecnología, permite la gobernanza en el mundo digital. Si bien se requiere de un marco legal para la regulación y supervisión de la infraestructura, también se debe retomar la concepción sobre derechos humanos y cooperar con las comunidades digitales para la especificación de las necesidades, creando políticas relacionadas que de alguna manera garanticen la protección del individuo en el ciberespacio.

Al mismo tiempo, algunas problemáticas como pobreza, violencia, brecha digital (debido a la desigualdad) han ocasionado que las redes sociales den una seguridad y permitan la comunicación entre individuos, pero siendo más vulnerables a la guerra digital que converge en un estado fragmentado de la gobernanza. Una crisis que lleva a impactar todos los ámbitos de la sociedad y lleva a la población de forma obligada a tener en cuenta las políticas estatales, regionales y mundiales sobre la ciberseguridad.

CAPÍTULO III: MARCO METODOLÓGICO

Según Hernandez Sampieri (2014): “La investigación es un conjunto de procesos sistemáticos, críticos y empíricos que se aplican al estudio de un fenómeno o problema” por lo tanto en el siguiente capítulo se expone la estructura de la investigación y los instrumentos que se van a utilizar para presentar el proceso enfocado al tema de investigación. El enfoque de la investigación es cualitativo ya que se utiliza un proceso de descripción y medición de variables sociales que van a ayudar con el análisis de la situación de la gobernanza costarricense dentro del ámbito de la ciberseguridad. A su vez, se toman las experiencias de Estados Unidos y México en el desarrollo de la seguridad nacional como referencia al estado en Costa Rica.

Con respecto al diseño, al esclarecer la pregunta investigativa, se utiliza el método descriptivo para demostrar como el estudio de las variables ha generado un impacto en la ciberseguridad. Las características compartidas entre los países de estudio, México, Estado Unidos y Costa Rica permite describir la situación en el Sistema Internacional del tema. Asimismo, que las variables crean un contexto de la fase en el que el gobierno de Costa Rica se encuentra con respecto al desempeño de la seguridad tecnológica.

La utilización de las distintas fuentes tanto primarias y secundarias plantea la confianza y la relevancia del tema para cada Estado. Se enfoca la visión de los actuales gobernantes con respecto a la ciberseguridad. Se presentan las estrategias nacionales en el tema, y los alcances deseados en cuanto a resguardo de los datos privados de los ciudadanos. La revisión bibliográfica y las entrevistas a profundidad permiten conocer la opinión de profesionales especializados y presentan la base teórica para desarrollar el tema investigado.

El desarrollo de las variables viene a denotar como los objetivos planteados en la investigación se observan y se analizan de acuerdo con la ciberseguridad y la situación actual en Costa Rica. La necesidad de extender el desarrollo de estas variables propone un escenario necesario para lograr entender el impacto de las TIC’s y su potencial en el resguardo de los datos.

3.1 Enfoque de Investigación

Según Hernández, Fernández y Baptista (2014) existen “dos aproximaciones principales de la investigación: el enfoque cuantitativo y el enfoque cualitativo”, sin embargo, ambos utilizan procesos metódicos y empíricos para la exposición de un tema. Es por esta razón que el enfoque de la investigación, al inicio puede ser mixta en tanto se estudia a profundidad un tema y se evalúan los fenómenos observados. El presente trabajo investigativo tiene un enfoque cualitativo.

El enfoque cualitativo, los mismos autores lo definen como aquel que “utiliza la recolección y análisis de los datos para afinar las preguntas de investigación o revelar nuevas interrogantes en el proceso de interpretación” por lo que las preguntas de esta pueden desarrollarse antes, durante o después de la recolección y análisis de los datos. Asimismo, “se basa en métodos de recolección de datos no estandarizados. No se efectúa una medición numérica, por lo cual el análisis no es estadístico.”

El enfoque cualitativo, también desde el punto de vista de Quecedo y Castaño (2002), implica que la investigación debe ser desarrollar conceptos que parten de las pautas de datos, con un estudio flexible; donde las personas no son únicamente variables sino se' considera el contexto y las situaciones en las que se hallan. Y se da énfasis a la validez de la investigación pues: “Aseguran un estrecho ajuste entre los datos y lo que realmente la gente hace y dice”. Donde se puede vislumbrar la posición del Gobierno de Costa Rica, mientras se ve con detalle el proceder de la ciudadanía alrededor de la protección y seguridad de los datos que se encuentran en el ciberespacio.

El enfoque cualitativo es especialmente relevante para evidenciar el estado de la gobernanza de la ciberseguridad en Costa Rica, nuestro eje fundamental en la investigación. Asimismo, este permite crear un escenario real con testimonios que se utilizaran en los instrumentos. En general, se logrará contextualizar mediante análisis de los marcos jurídicos, tecnológicos y educativos de otros países como Estados Unidos y México, el avance que nuestro país ha tenido en este tema.

3.2 Diseño de la Investigación

El desarrollo del presente trabajo debe contestar concretamente la pregunta fundamental para la investigación referente a la gobernanza y la ciberseguridad, y cumplir con los objetivos que se han fijado. Los estudios cualitativos facilitan la interpretación de datos empíricos no estandarizados que dan descripciones de las interacciones ciudadanas de nuestro tema. De esta forma se plantea la profundidad del escenario que se propone trazar con el desarrollo de la concepción estatal de la ciberseguridad.

El diseño de la investigación indica Hernández, Fernández y Baptista (2014) que "se refiere al plan o estrategia concebida para obtener la información que se desea con el fin de responder al planteamiento del problema". El resultado va a depender según la precisión, amplitud y profundidad de la información obtenida. Los componentes del proceso, las variables, van a extender el escenario de la protección de las TIC's y paralelamente el estado en el que el gobierno de Costa Rica maneja la normativa y desarrollo de las especializaciones alrededor del mismo.

La presente investigación tiene un diseño descriptivo puesto que busca especificar las características del fenómeno de la ciberseguridad dentro de los alcances estratégicos del gobierno de cada caso estudiado: México, Estados Unidos y Costa Rica. Esta clasificación va de la mano con lo entendido previamente, en donde se recoge información sobre las variables a las que se hace referencia. Se debe tener en cuenta con claridad que existen limitaciones que no podrán extenderse como variables del tema.

La utilidad que presenta este tipo de diseño se basa en la precisión con la que se muestran ángulos de un fenómeno o situación. Por ello, se visualizan los conceptos y variables relacionadas al objetivo general de la investigación. Donde el grupo que se procura estudiar está relacionado a la sociedad costarricense y a las entidades gubernamentales que regulan la seguridad cibernética. Asimismo, como los planes educativos especializados que generan un impacto en la defensa contra los crímenes tecnológicos.

3.3 Fuentes de Información

La información es básica para constituir el progreso de una sociedad, y es indispensable conocer las características de esta para poder abordar cualquier proceso de documentación. Cid y Perpinyà (2013) define la información como:

> "Un conjunto de datos ordenados e interrelacionados en un contexto determinado y es la base del conocimiento. La misma información puede tener valores diferentes según quien la posea. Además, no tiene valor alguno mientras no sea utilizada; en este sentido, no es un fin en sí misma, sino un medio para conseguir algo." (p. 11)

En el afán de la documentación, la revisión bibliográfica es una de las fuentes que se considera necesaria para recopilar la información para enmarcar el problema de investigación. La compilación debe ser selectiva según importancia y vinculación al planteamiento del problema. Asimismo, deben ser publicaciones recientes para darle validez empírica. Otro tipo de fuente se refiere a entrevistas a profundidad, grupos de enfoque o creaciones culturales mediáticas.

3.3.1 Fuentes primarias

Hernández, Fernández y Baptista (2014) indica que las fuentes primarias "proporcionan datos de primera mano, pues se trata de documentos que incluyen los resultados de los estudios correspondientes". Este tipo de fuentes incluye libros, tesis y testimonios de expertos. La recomendación de estos autores es iniciar consultando uno o varios especialistas en el tema investigado.

En el caso de revisión bibliográfica se establece una secuencia de los hechos y su contexto de forma que sistematizan la información. Con los testimonios, o entrevistas a profundidad, estas son flexibles y dinámicas. Según Taylor y Bogdan, citados por Quecedo y Castaño (2002), las entrevistas son "encuentros dirigidos a la comprensión de las perspectivas que tienen los informantes de sus experiencias o situaciones, tal como las expresan con sus propias palabras".

Para la investigación, se utilizará tanta revisión bibliográfica de las Estrategias Nacionales de la Ciberseguridad de Estados Unidos, México y Costa Rica y documentos de entidades gubernamentales relacionadas al impacto de las TIC's. También se consultará a expertos en la forma de entrevistas de profundidad, para tener una visión más amplia sobre el contexto nacional en relación con tres pilares: normativo, presupuestario y de programas educativos especializados.

3.3.2 Fuentes secundarias

Las fuentes secundarias de la información forman parte de la revisión bibliográfica. Estos consisten en compilaciones, referencias, alrededor del tema de investigación. Este se puede utilizar para acceso a las fuentes primarias. También poseen el procesamiento de la información de una fuente primaria.

La investigación utilizara distintas fuentes secundarias a partir de análisis comparativos alrededor de tecnologías de información y ciberseguridad. Estos artículos han procesado los datos de las entidades gubernamentales o de otros sectores poblacionales en donde se da relevancia a las tecnologías de información y al auge en la protección cibernética.

3.4 Variables o Categorías de Análisis de la Investigación

El concepto de una variable se aplica a la investigación para darle valor a la hipótesis o planteamiento del problema. Como Hernández, Fernández y Baptista (2014) propone "es una propiedad que puede fluctuar" aplicable a "objetos, hechos y fenómenos, los cuales adquieren diversos valores".

En el caso de la investigación cualitativa, este se refiere a propiedades de los objetos de estudio, determinando la presencia de esta. Para la presente investigación, se propone el análisis de categorías de acuerdo con los objetivos:

Cuadro 2. Presentación de las variables de la investigación

Objetivo	Variable	Definición Conceptual	Definición Operacional	Definición Instrumental
Reconocer la evolución de los desafíos relacionados a las tecnologías de la información.	Crímenes relacionados a las tecnologías.	Los crímenes de las tecnologías, o cibercrímenes, son reconocidos como conductas criminales que atentan contra la confidencialidad y la integridad de los datos. De manera relevante, desde la introducción de los sistemas computacionales han existido eventos pivótales en la forma que se entienden y desarrollan los cibercrímenes.	Desarrollo Histórico.	Revisión Bibliográfica.
Detallar las políticas de seguridad nacional que utilizan actualmente Estados Unidos y México en cuanto a ciberseguridad.	Políticas de Seguridad Nacional (ciberseguridad).	Seguridad Nacional es concebida como el accionar de un Estado frente a riesgos o acciones maliciosas en el ámbito físico o tecnológico. Esto implica el uso de estrategias de respuesta para contrarrestar las acciones. De igual forma, la Seguridad Nacional es la protección proactiva de la población para resguardar tanto la seguridad física como la protección de información que evite el mal uso de datos privados estatales o personales (ejemplo espionaje, robo de identidad).	Desarrollo militar de la estrategia de ciberseguridad para Estados Unidos. Desarrollo humanista de Latinoamérica con enfoque en México sobre la ciberseguridad.	Entrevista a profundidad.

Identificar el estado de la gobernanza en Costa Rica en torno a la legislación de las tecnologías de seguridad de la información.	Gobernanza en Costa Rica.	La concepción de la gobernanza se va a analizar desde dos ejes temáticos: - La forma jurídica de gobernar un Estado y el impacto que tiene la normativa en la vida cotidiana de los ciudadanos - La forma en la que un Estado influencia a la población indirectamente mediante el uso de inmersión de tecnologías en distintos aspectos relevantes como educación e infraestructura.	Legislación y apertura a la especialización del sector de seguridad cibernética.	Entrevista a profundidad.
Analizar el impacto de la ciberseguridad en la gobernanza.	Impacto de la Ciberseguridad en la cotidianeidad.	El impacto de la protección de datos en el ciberespacio (ciberseguridad) debe considerar la responsabilidad de los gobiernos, la cooperación interestatal y la cooperación con el sector privado para poder salvaguardar al usuario final, o sea el ciudadano. Los pilares fundamentales para la ejecución de la normativa conllevan desafíos y riesgos educativos, estructurales e institucionales.	Desarrollo de la gobernanza para la Sociedad Digital. Vulnerabilidades, riesgos y amenazas vigentes en Costa Rica.	Entrevista a profundidad.

3.5 Instrumentos de la investigación

Los instrumentos de medición según el aporte de Hernández, Fernández y Baptista (2014) son el “recurso que utiliza el investigador para registrar información o

datos sobre las variables que tiene en mente" de manera que se pueden registrar datos para la representación de las variables de forma confiable. La recolección de la información se va a llevar a cabo técnicas como revisión bibliográfica, cuestionarios y entrevistas.

3.5.1 Instrumento #1. Línea de tiempo

Objetivo: Reconocer la evolución de los desafíos relacionados a las tecnologías de la información.

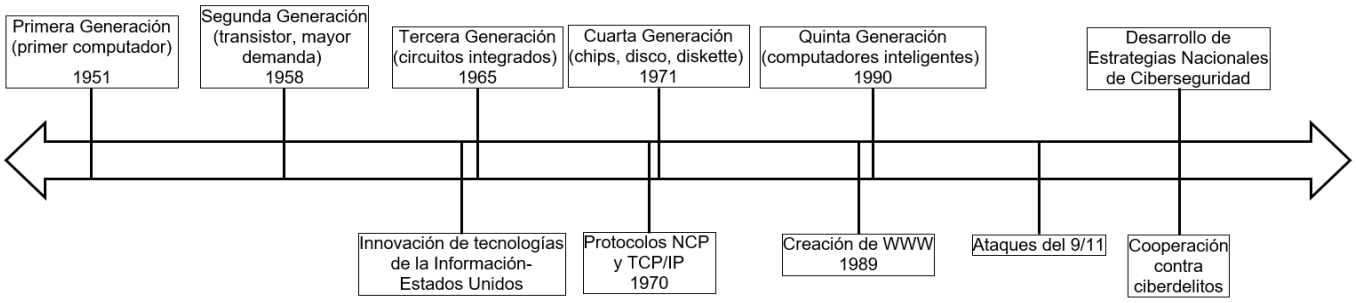

Figura 1. Elaboración propia con base al libro Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare (2015).

3.5.2 Instrumento #2. Entrevista a profundidad

Objetivo: Detallar las políticas de seguridad nacional que utilizan comúnmente Estados Unidos y México en cuanto a ciberseguridad.

1. A nivel estatal, ¿cómo definiría usted la cultura de protección de información/datos en Costa Rica?
2. ¿Cuál es su opinión con respecto a la ciberseguridad en las entidades públicas? ¿Cómo se podría agilizar la digitalización (el Gobierno Digital) con el fin de tener una política de ciberseguridad para el Estado?
3. Me puede comentar: ¿Cuál es el estado actual de la infraestructura critica en el país?
4. De acuerdo con la seguridad cibernética de países como Estados Unidos, las Iniciativas han derivado del trabajo en conjunto con el sector militar, mientras que

en Costa Rica la creación de políticas públicas ha derivado de los derechos fundamentales de los usuarios, ¿Cómo ve el futuro de la ciberseguridad en la región?

3.5.3 Instrumento #3. Entrevista a profundidad

Objetivo: Identificar el estado de la gobernabilidad en Costa Rica en torno a la legislación de las tecnologías de seguridad de la información.

1. Según el BID y otras entidades internacionales, la protección de datos debe ser garantizada ¿considera que en Costa Rica esto se cumple de manera eficiente y transparente? ¿Por qué?
2. ¿Cuál es la posición estatal frente a la especialización en el sector con respecto a apertura de puestos en las distintas entidades? ¿Se está tomando en cuenta las necesidades futuras?
3. En Costa Rica la creación de políticas públicas sobre TIC's y seguridad cibernética ha derivado de los derechos fundamentales de los usuarios, ¿Cómo ve el futuro de la ciberseguridad en la región y en el país?
4. Dentro del marco de la ciberseguridad, encontramos una serie de delitos como hackeo, piratería, correos electrónicos con información falsa (phishing), entre otros. ¿Qué modificaciones o actualizaciones se le debe hacer a la legislación costarricense para enfrentar riesgos o amenazas?

3.5.4 Instrumento #4. Entrevista a profundidad

Objetivo: Analizar el impacto de la ciberseguridad en la gobernanza.

Contextualización: Para desarrollar el termino TIC se tomará en cuenta la definición: "*Es el conjunto de herramientas, soportes y canales desarrollados y sustentados por las tecnologías (telecomunicaciones, informática, programas, computadores e internet) que permiten la adquisición, producción, almacenamiento, tratamiento, comunicación, registro y presentación de informaciones, en forma de voz,*

imágenes y datos, contenidos en señales de naturaleza acústica, óptica o electromagnética a fin de mejorar la calidad de vida de las personas"

1. ¿Qué tan frecuentemente utiliza las tecnologías de información? ¿Considera usted que los costarricenses han adoptado el uso de las TIC's? Por favor, explique.
2. Siguiendo con la temática de la tecnología, ¿considera que los costarricenses tienen un buen uso de los conceptos de privacidad y protección de los datos? ¿por qué?
3. ¿Cuál es su opinión con respecto a la ciberseguridad en las entidades públicas? ¿Cómo se podría agilizar la digitalización (el Gobierno Digital) con el fin de tener una política de ciberseguridad para el Estado?
4. Dentro del marco de la ciberseguridad, encontramos una serie de delitos como hackeo, piratería, correos electrónicos con información falsa (phishing), entre otros. Si pudiese hacer una propuesta legislativa al respecto, ¿en qué tema se centraría? ¿Considera usted que estos delitos son fáciles de identificar?

3.6 Recolección y procesamiento de Datos

Para la recolección de datos se utilizará: línea de tiempo y entrevistas a profundidad. De forma que se logre exponer con detalle la información para cada objetivo de acuerdo con el tema investigado.

3.6.1 Recolección de Datos Instrumento #1. Línea de tiempo

Se realizará una línea de tiempo que indique con claridad los eventos que se han clasificados de impacto histórico como cibercrímenes.

1. Década de 1970: Auge del uso de los sistemas computarizados debido a avances en los equipos (hardware) y velocidad del sistema. Estos progresos evolucionan de daños físicos al equipo a uso ilegal de las computadoras en la manipulación de datos, entendido como fraude.

2. Década de 1990: Evolución de los computadores personales, comercialización de impacto entre procesadores personales. Desarrollo inherente del software y los crímenes relacionados como piratería, robo de patentes y virus cibernéticos, a su vez empieza el anonimato de los crímenes al poder conectarse de forma remota a los sistemas. Lanzamiento del World Wide Web que facilita el intercambio de información y desafía la normativa estatal frente a restricciones, los crímenes electrónicos se transforman a crímenes transnacionales cibernéticos.
3. Ataques del 9/11: El impacto del ciberterrorismo y el uso de las TIC's en conflictos armados denotan un punto de inflexión en el uso de la tecnología, no solo como sistema de información, sino como arma de los Estados y otros grupos. El enfoque de la discusión de la ciberseguridad se torna hacia la comunidad internacional al entender que los desafíos deben tener soluciones y normativa en conjunto de los Estados.
4. Auge de las TIC's: Entre el 2007 y el 2008, países como Estonia y Georgia recibieron ataques cibernéticos en las entidades estatales y empresas privadas. La incapacidad de determinar el punto de origen de los ataques hace que las políticas para establecer los delitos se dificulten. La dependencia de las TIC's hace que los sistemas y los servicios sean más vulnerables a los ataques contra infraestructuras críticas.
5. Estrategias Nacionales de Ciberseguridad: Generación de foros internacionales y estrategias estatales para habilitar de forma efectiva la ciberseguridad. La armonización de leyes es vital, sin embargo, se debe tener en cuenta la capacidad de adaptación de cada Estado.

3.6.2 Recolección de Datos Instrumento #2. Entrevista a profundidad

La entrevista a profundidad relacionada a las políticas de seguridad nacional se efectuó a un ingeniero de sistemas con especialización en ciberseguridad, está al tanto del contexto regional y local en cuanto a las medidas de seguridad referentes en la Estrategia Nacional de Ciberseguridad. Se relacionaron las preguntas a la actualidad del país, la cibercultura del costarricense y el futuro de la ciberseguridad como parte de la estrategia de digitalización nacional.

Se indican 4 puntos principales en la entrevista:

1. Los adelantos tecnológicos traen implícitos retos en la ciberseguridad, y los Estados si bien tienen un presupuesto asignado, este es invertido usualmente en infraestructura y aplicaciones que ayudan a resguardar y acceder la información de las instituciones públicas. Sin embargo, se tiene un débil programa de capacitación a los usuarios que los cibercriminales aprovechan.
2. Costa Rica está ampliando sus fronteras frente a la digitalización, por medio del MICITT y CSIRT, 4 ingenieros velan por la ciberseguridad de las instituciones públicas. Sin embargo, el personal asignado a esta tarea es deficiente frente a 342 instituciones en el país. Se deben clarificar procedimientos de comunicación, validación y ejecución ante una posible amenaza.
3. En muchas ocasiones, los ciberataques buscan de desestabilización de un país. El reconocer las amenazas, abordarlas de forma colectiva y comprender que se necesitan soluciones integrales, abre una posibilidad para desarrollar un enfoque de ciberseguridad unificado; para proteger a las infraestructuras críticas de las que dependen los ciudadanos.
4. Históricamente, se ha demostrado que las iniciativas lideradas por el sector privado o militar pueden movilizarse más rápidamente a través de alianzas público-privadas y marcos de colaboración que promueven la gobernanza, los roles y las responsabilidades, los estándares, el intercambio de inteligencia de amenazas y mejores prácticas

3.6.3 Recolección de Datos Instrumento #3. Entrevista a profundidad

La entrevista a profundidad relacionada al marco jurídico se efectuó a una técnica en ciencias forenses con especialidad en ciberseguridad. Se trataron los temas de la legislación actual y los desafíos regionales y locales alrededor del cumplimiento de este marco. Ella resalta los siguientes puntos:

1. Al ser un tema no sólo de manejo técnico sino legal, las implementaciones jurídicas se van generando a medida que los cambios sociales así lo ameriten para regular y proteger las interacciones.
2. Con el CSIRT, el Estado ha dado atención a los temas de ciberseguridad, en cuanto a seguridad y vulnerabilidades mas no así en el manejo de la información. Esto ha quedado pendiente en las facultades de la PRODHAB.
3. Aún hay camino por recorrer desde la institucionalidad ya que tradicionalmente en temas de ciberseguridad el sector privado transnacional ha ido a la vanguardia.
4. Con el desarrollo de la Estrategia Nacional de Ciberseguridad y la suscripción a la Convención de Budapest se han ido actualizando las tipificaciones delictivas cibernéticas permitiendo el avance.

3.6.4 Recolección de Datos Instrumento #4. Entrevista a profundidad

La entrevista a profundidad relacionada al estado de la gobernanza se efectuó a un periodista, psicólogo con estudios en Ciencias Políticas. Se escogió a este profesional para ampliar el criterio de la gobernanza digital y la perspectiva de los usuarios de forma que permite tener una opinión no especializada sobre la ciberseguridad y su impacto.

Los puntos más relevantes que menciona:

1. El uso de los dispositivos celulares permite el acceso a internet en la gran mayoría de la población. Sin embargo, al compartir libremente datos personales en las redes sociales; sin revisar los acuerdos del uso de estos, o compartir conversaciones privadas se están cometiendo delitos. De igual manera, se observan los casos de estafas que han ido en aumento.
2. Las entidades públicas tienen un manejo precario del tema de privacidad y seguridad de la información que resguardan, esto ha sido señalado en múltiples ocasiones por parte de auditorías de la Contraloría General de la República.
3. La legislación debería no solo tipificar los delitos, sino también garantizar los recursos necesarios para que los organismos competentes tengan las

herramientas, tanto materiales como de capital humano, para perseguir esos delitos.

CAPÍTULO IV: ANALISIS DE RESULTADOS

El análisis de los resultados plantea la extracción de los conocimientos sobre la realidad del problema de la investigación. En este caso, realizar una recopilación de datos en su mayoría cualitativos que representan posturas académicas e ideológicas alrededor de la gobernanza de la ciberseguridad en Costa Rica. El análisis es posible debido a una idea que genera una profundización de un tema y esta se condensa para darle un significado, categorías y conclusiones o recomendaciones posteriormente.

La codificación de los resultados presentados a continuación se realizó por medio de una revisión bibliográfica, entrevistas a expertos y subsecuentemente consideraciones de los hallazgos almacenados. La digitalización del Estado y la posición de gobernanza tanto física como virtual, plantean beneficios y desafíos en la Sociedad de la Información. A través de la revisión de los antecedentes bibliográficos sobre las Tecnologías de la Información, la Estrategia de Ciberseguridad de México, Estados Unidos y Costa Rica y el estado del marco normativo costarricense se expone como los crímenes del Siglo XXI afectan a Costa Rica.

Con respecto a los avances tecnológicos y la acogida de parte de los gobiernos de Costa Rica, se pueden hacer comparaciones con respecto al fenómeno global. La forma de vislumbrar la fragmentación de la sociedad y los riesgos y amenazas que surgen de la Sociedad del Riesgo permiten caracterizar la gobernanza digital y el impacto para el crecimiento de la población costarricense. A su vez, ejemplificar los datos encontrados con la síntesis de las entrevistas a expertos crea un balance para la formulación de los resultados.

El presente capítulo pretende esclarecer por medio del análisis la posición actual de la gobernanza y la ciberseguridad en Costa Rica, un tema que necesita una revisión como visión de país, y con un potencial innovador significativo en la región. Una oportunidad para priorizar algunos ejes de trabajo que facilitan la vida en una comunidad virtual.

4.1 Evolución de los desafíos de las Tecnologías de la Información

Los desafíos de las Tecnologías de la Información son presentados de forma cronológica por medio de una matriz documental donde los principales indicadores de la evolución de la tecnología se subdividen en generaciones y los desafíos derivados del fenómeno de la globalización. Este instrumento busca analizar los acontecimientos de aproximadamente 70 años de desarrollo. Los crímenes del Siglo XXI se identifican como la falta de protección a los derechos del individuo en el ciberespacio y por consecuente los efectos que tiene en la Sociedad de la Información, estos eventos llevan a un cambio en el actuar de los Estados frente a una crisis de identidad emanada de un nuevo mundo.

La matriz documental detalla con claridad como Estados Unidos y los diferentes Estados u organizaciones interestatales llegan a una revolución digital, de manera incipiente, que permite ampliar las formas de comunicación abriendo el ciberespacio a todas las personas. Inicialmente, la creación del computador da acceso al desarrollo de sectores que impulsan tecnología, transporte, ciencia, entre otros. Poco a poco, la necesidad y el crecimiento que supone la comercialización de las TIC’s llevo a la creación de políticas y protocolos que permitieran la comunicación eficaz inclusive entre diferentes instrumentos tecnológicos.

Junto con el desarrollo y alcances beneficiosos para la sociedad, los actores estatales encuentran las facilidades estratégicas de las nuevas tecnologías y su utilización en el campo militar se enfoca en dos áreas: infraestructura/componentes y uso de la información para promover agendas políticas en la sociedad. Inclusive, se puede exponer el uso fuera del marco jurídico de la tecnología para facilitar operaciones militares. Otros actores ven en las TIC’s, el arma para contraponerse a las agendas militares y de control del poder de las potencias como Estados Unidos y Europa. La generación de ataques se expande más allá del espionaje; cuando la organización y planificación del 9/11 se vislumbra como un ataque terrorista propiciado por las TIC’s.

La creación de las estrategias nacionales de ciberseguridad deriva directamente de la respuesta de los países ante las amenazas y vulnerabilidades potenciales después

del fenómeno 9/11. Si bien se plantean iniciativas con una base de estrategia militar para el control del ciberespacio y de las TIC's, como es el caso de los Estados Unidos. En la región latinoamericana se observa un enfoque distinto con mayor arraigo en los derechos fundamentales y la cooperación para la prevención y sanción de crímenes cibernéticos.

Cada paso tecnológico alrededor del desarrollo eficiente de las tecnologías computacionales y posteriormente cibernéticas ha brindado beneficios y desventajas, las cuales han marcado la respuesta de expertos, políticas e incluso otros ciber delincuentes en torno al uso de medidas de ataque a los instrumentos que permiten el funcionamiento de las TIC's. A partir de la década de los 80, código malicioso ha sido encontrado en diferentes equipos. Con la creación de World Wide Web, los códigos y aquellas personas que los desarrollan saltaron a infección por medio de correos electrónicos aumentando la complejidad de rastreo y de maneras creativas para infectar los sistemas, especialmente de Windows. Desde el uso de documentos en Word o Excel, hasta tratar de asaltar la Casa Blanca por medio de un ataque de DDoS.

La agilidad y la rapidez de la formulación de nuevas formas de contaminar el ciberespacio fue una fuente de preocupación para los Estados, principalmente para Estados Unidos, cuyos gobiernos han utilizado este fenómeno de cibercrimen para contraatacar a los potenciales hackers y utilizar la tecnología contra otros gobiernos, permitiendo acceder a información privilegiada o simplemente para causar desinformación en la ciudadanía. El desarrollo de la criminalidad ya no es solo para computadores o para disminuir las ganancias económicas en cierta industria, sino que tiene un impacto de billones de dólares al año en las economías más grandes del planeta.

Al utilizar las TIC's como parte de la estrategia militar, en diferentes ocasiones, la versatilidad de estas ocasiona una contraposición que acabaría definiéndose como parte del terrorismo. Si bien, el tema no trata el auge del terrorismo cibernético, como WikiLeaks o Anonymous, si representa un cambio en la visión de la seguridad nacional para los Estados y organizaciones interestatales; de manera que se empieza a hacer una medición más exhaustiva de los detrimentos de los ataques, más allá de los términos económicos. Por ejemplo, el auge de las TIC's en la sociedad, que tan conectado y a

que plataformas se conectan los individuos, cual es el costo de utilizar la tecnología de un país a otro, etc. La modernidad liquida y la manera de llevar acabo las estrategias con métodos digitales enfocan el posicionamiento del poder en la Guerra Digital.

De manera paralela a la Guerra Digital, esfuerzos internos de Estados Unidos llevan a la innovación con un instrumento llamado “unión router” debido a las diversas capas de encripción permite la aparición de la llamada “Deep Web” (DW). Johnson (2015) lo califica como aquel que “*tenía el propósito de permitir a la policía, milicia, y organizaciones gubernamentales utilizarlo para llevar a cabo sus negocios en un modo privada o para inteligencia y operaciones encubiertas*.” Sin embargo, la Deep Web fue descubierta por ciber criminales y otros actores que la usan para actividades ilegales desde venta de drogas hasta pornografía infantil.

La fragmentación de la sociedad y la dialéctica del ciberespacio y el Internet como actores con poder globalizador convergen en la manera que se han efectuado los avances tecnológicos de forma desigual. La retrospectiva que deja un evento como la medición de la Guerra Digital en la sociedad es un indicativo de la flexibilidad, maleabilidad del colectivo y la individualización del espacio que permite la desinformación y los medios de comunicación para el fomento de la guerra, el auge del poder político frente a necesidades en una realidad paralela fuera del ciberespacio.

Por otro lado, la DW es un ejemplo de cómo la estrategia militar fracasa y en última instancia la iniciativa es absorbida en la Sociedad del Riesgo, incrementando la desconfianza y las irregularidades que se pueden llegar a presentar fuera de los limites gobernables de un Estado. ¿Qué influencia tiene cualquier gobierno frente a una amenaza invisible, con actores del ciberespacio, con igual cuota de poder? Es una de las interrogantes que dan cabida a la formación de estrategias de ciberseguridad nacional.

Un evento que presume el cambio en la sociedad y la visión sobre el impacto de las TIC’s son los ataques terroristas del 11 de Setiembre en Estados Unidos. Este evento en particular genero una serie de iniciativas y conversaciones sobre el estado de la

Sociedad de la Información, las ventajas comparativas de los ataques coordinados en una estrategia mixta y el terrorismo expansivo a nivel global. Despliega características que demuestran la crisis de la gobernanza de los Estados tanto en el plano “real” como en el “virtual”.

La detección de las vulnerabilidades y amenazas se volvió una prioridad para Estados Unidos, incentivando la creación de una estrategia nacional de ciberseguridad. El presupuesto federal asignado para la iniciativa concentra a instituciones militares como eje principal en el desarrollo de las políticas públicas para la protección de la información estatal. A su vez, la actual estrategia detalla la proliferación de las TIC’s en la sociedad y la necesidad de proteger los datos personales de los ciudadanos.

Para el gobierno estadounidense, el impacto financiero, social y político de la falta de protección de los datos que transitan en el ciberespacio tiene una connotación de control frente a otros actores. Parte de las preocupaciones que han surgido en este tema lo conforma el accionar proactivo del Estado frente a estrategias de ciber espionaje o los ya mencionados ciber ataques al sector privado. Estados Unidos pretende mantener el puesto de innovación tanto tecnológica como cooperativa de regulaciones en el ciberespacio que le den cierta gobernanza interestatal y proteja la digitalización de las entidades gubernamentales.

La fragmentación en la Sociedad de la Información ha llevado consigo una crisis para los Estados y las instituciones intergubernamentales. Por un lado, la penetración de las TIC’s en la sociedad fortalece la teoría de comunidades digitales, creación de espacios cibernéticos y digitalización del Estado como parte de una agilización de procesos y mejor comunicación entre instituciones públicas y los ciudadanos. Aceptar, planificar y desarrollar la infraestructura pública para los gobiernos digitales a nivel global ha sido un desafío de presupuesto y especialistas, si, ha generado nuevas especializaciones y formas de educación, pero deriva en una crítica hacia la manera de la formación de alianzas interestatales.

Estados Unidos tiene claro que la cooperación entre los diferentes gobiernos facilita la comunicación de técnicas de ciberdelitos y listas de posibles ciberdelincuentes, más allá ayuda en la Guerra Digital y el enfoque antiterrorista de la nación. En el caso de América Latina, enfatizado en México y Costa Rica, la creación de CSIRT, que son los centros de respuesta ante vulnerabilidades y amenazas, permite la constante comunicación y cooperación especializada enfocada en la ciberseguridad. Los 3 países forman parte de una red que incentiva los análisis de la gobernanza digital, y recalca el rol de inteligencia por ejemplo de las entidades estadounidenses para la formación de profesionales.

4.2 Estrategias de Seguridad Nacional para Estados Unidos y México en materia de ciberseguridad

Las iniciativas gubernamentales frente a la ciberseguridad se determinan por medio de la Estrategia de Ciberseguridad de cada Estado, estas tienen como objetivo resguardar tanto al país como a los ciudadanos. Para la protección de los datos internos que los gobiernos digitales poseen se deben crear diferentes planteamientos a nivel jurídico. En cuanto a la protección de los datos personales de los ciudadanos, mediante campañas en distintos sectores como educación y mercadeo permite incentivar el conocimiento alrededor de los cibercrímenes de nuestra actualidad.

Para analizar las estrategias, se realizó una entrevista sobre la Estrategia de Ciberseguridad, así como de la actualidad del país y su aplicación a un experto en ciberseguridad con conocimiento de infraestructuras críticas, políticas públicas e instituciones de seguridad cibernética. A su vez, se realizó una revisión bibliográfica para complementar los datos obtenidos mediante la entrevista. Esta revisión permite ampliar los conceptos e información respectiva a las estrategias de Estados Unidos, México y Costa Rica.

Cuadro 3. Estrategias de Ciberseguridad de los casos de estudio: Costa Rica, México y Estados Unidos.

Costa Rica	**México**	**Estados Unidos**
Estrategia Nacional de Ciberseguridad creada en 2017. El MICITT con la figura del CSIRT es la institución que se encarga del desarrollo de las políticas públicas relacionadas con las telecomunicaciones. La Agencia de Protección de Datos de los Habitantes (PRODHAB) ayuda a otras instituciones gubernamentales en la agilización de datos, control y protección. Se pueden presentar denuncias en el espacio de la cibernético que judicialmente carecían de respuesta. Plantea mejoras en el desarrollo de las TIC en sectores como salud, seguridad ciudadana, educación, cultura, comercio y gobierno digital.	Estrategia Nacional de Ciberseguridad de México creada en el 2017. Tiene como finalidad la digitalización en donde se expone la brecha digital de protección al no tener una Agencia de Ciberseguridad Nacional que incentive la gobernanza digital, definición de un marco jurídico que tenga en cuenta leyes federales y estatales y protección de infraestructura critica. Defensa cibernética a cargo de las Fuerzas Armadas.	Estrategia Nacional Cibernética creada en 2018. El impacto financiero, social, gubernamental y político que tienen las TIC's es evidente frente a la estrategia de los competidores directos (ciberespionaje y actividades maliciosas) Estados Unidos propone: 1. Cooperación: Fomento de la ciberresiliencia junto con el sector privado 2. Sanciones económicas para actores que realicen actividades maliciosas Fomenta la protección del pueblo estadounidense, seguridad nacional y formas de vida de la sociedad.

Fuente: Elaboración propia con base en la Estrategia Nacional de Ciberseguridad.

Las estrategias de seguridad cibernética se han creado, de manera general, para proteger a la sociedad de amenazas y fomentar la bienestar económico, social, cultural basado en el impacto de las TIC's. Esta digitalización de la sociedad ha tenido que verse armonizada con los valores y derechos fundamentales como la libertad y la privacidad. La innovación estructural detrás de la utilización de las TIC's ha permitido que Internet y el ciberespacio sean herramientas que proveen apertura y universalidad dándole

confianza a los ciudadanos sobre las TIC's y sobre la conceptualización de la ciberseguridad.

En el caso estadounidense, este país ha sido pionero en la innovación y adquisición de tecnología que le permita: mantener protagonismo mundial y control sobre los conflictos internos o externos que le sean de interés. Es, por tanto, que la noción sobre la participación de los militares e inteligencia del gobierno se encuentra claramente descrita en la Ciberestrategia Nacional. El enfoque especifico de esta iniciativa se concentra en aspectos internos que le agreguen valor al uso de las TIC's, la infraestructura, innovación y economía digital mientras que provean una posición de cooperación internacional enfocada en la protección y sanción de las actividades maliciosas en el ciberespacio fomentando la necesidad del peso que lleva el país en cuanto a influencia en políticas o convenios internacionales.

México, se encuentra en un puesto muy distinto al de Estados Unidos. El gobierno reconoce la necesidad de crear una Estrategia Nacional de Ciberseguridad, debido al impacto económico que sufre el país al poseer vulnerabilidades, riesgos y amenazas que permiten los ciberdelitos. Sin embargo, se enfatiza la protección de la dignidad humana, el patrimonio del sector empresarial (privado o público) y la seguridad nacional; es ese orden. Una visión desde la concepción que en la región representa un nuevo paradigma y un punto de equilibrio entre la necesidad de protección del aparato de gobierno o de control sobre otros y la defensa que se le debe dar a los ciudadanos. Por ello, la iniciativa se basa en derechos humanos, gestión de riesgos y colaboración multidisciplinaria.

Para el Estado mexicano, cabe recalcar que las Fuerzas Armadas y la División Científica de la Policía Federal se encargan de la investigación de delitos cibernéticos. Parte del planteamiento de la iniciativa se debe a la falta de un marco regulatorio real que se está trabajando como hoja de ruta entre diferentes actores en el país. Esto implica el dialogo y creación de políticas públicas que realmente se enfoquen en el cuido de los datos desde la mayor cantidad posible de sectores. Un segundo paso en este camino incluye la promoción de la digitalización como parte del crecimiento económico del país.

En Costa Rica, la Estrategia Nacional de Ciberseguridad ha apostado por promocionar el uso de las TIC's para impulsar el desarrollo en sectores como salud, seguridad ciudadana, educación, cultura, comercio y gobierno digital. La iniciativa se concentra en el equilibrio en la incorporación de tecnología tanto para el sector público como privado, donde la eficiencia y el costo deben ser beneficiosos para los ciudadanos. Mientras que el panorama previo al lanzamiento de la iniciativa era calificado como insuficiente para la protección de amenazas cibernéticas, la penetración y protección de los datos ha ido cambiando en los años recientes. A pesar de la fragmentación entre el espacio físico y el ciberespacio hay algunas problemáticas que inciden en la protección de los ciudadanos: la brecha social que se traduce a brecha digital.

Las estrategias de seguridad nacional (ENCS), en algunas regiones, tienen un enfoque integral que incluye ámbitos de la vida gubernamental; económicos, educativos, sociales y los militares. La gobernabilidad entorno a la formulación de políticas de ciberseguridad usualmente están principalmente en las manos del sector militar y de inteligencia del gobierno. Sin embargo, concentrar la seguridad cibernética entorno a una estrategia militar, como parte de una guerra digital, pierde el enfoque sobre los derechos fundamentales como la libertad de expresión y la privacidad por lo que es importante tomar en cuenta la forma en que cada Estado desarrolla sus relaciones internacionales y la gobernanza del ciberespacio.

Se puede encontrar un contraste entre las ENCS que hace distinción entre la madurez del Estado y los recursos económicos y humanos concedidos para la seguridad cibernética. Si bien, Estados Unidos capta áreas como la innovación tecnológica y recursos económicos, es claro que el país tiene un nivel mucho mayor de madurez que el resto del continente. El hecho que la ENCS estadounidense no sea innovadora en cuanto a temática, deja en claro 3 puntos:

1. El país tiene más de 20 años trabajando en diferentes estrategias que protejan los datos que el gobierno genera, maneja y comparte.
2. Las alianzas público-privadas generan una cantidad de información relevante para la ciberseguridad y son las entidades militares quienes lo administran para

diferentes fines estratégicos, ya sea a nivel internacional o para generar algún impacto comercial a nivel interno. Las alianzas en telecomunicaciones en este sentido son esenciales.

3. El modelo de gobernanza estadounidense pretende ser expandido al ciberespacio, manteniendo la posición y poder de este país. Asumiéndolo como un desafío de liderazgo que se replica en otras latitudes.

En cuanto a América Latina, especialmente México y Costa Rica, representan realidades dentro de la misma vertiente integral. Las ENCS plantean políticas recientes que en algunos casos ejemplifican el estudio inicial de una problemática que no había sido tomada en cuenta por la cotidianeidad del Estado. En México, la presentación de la necesidad de entidades estatales para la regulación se encuentra inclusive en un estado más incipiente que el de Costa Rica. Una de las mayores dificultades para ese país es la falta de coordinación entre el Estado y el sector privado, así como la desigualdad imperante en la población que genera una deficiencia en el conocimiento y ejecución en la sensibilización alrededor de la protección de datos.

El caso de Costa Rica presenta la particularidad de no tener un ejército, lo cual más bien permite la búsqueda de soluciones teniendo como prioridad los derechos humanos, ampliamente expresado en la ENCS. Sin embargo, para el experto consultado del tema esto hace que la estrategia pierda fuerza y objetividad en cuanto a la necesidad de protocolos y definición de amenazas y vulnerabilidades. El Estado requiere una estrategia con mayor balance que permita visualizar con mayor claridad la importancia para el país, para la protección de datos en un gobierno con más de 300 instituciones públicas y con recursos limitados.

La eficiencia de las ENCS debe ser considerada en conjunto con distintas variables: gobernanza digital, marco jurídico, accionar de las instituciones y estado de la cooperación interestatal. Los países comparados tienen en común la creación de los Centros de Respuesta a Incidentes de Seguridad Informática (CSIRT) que se encarga de administrar y gestionar los incidentes informáticos de alto impacto para tener una reacción efectiva a las posibles amenazas. Los CSIRT forman una red regional en la que

además se comparte la información sobre vulnerabilidades y poseen expertos que extienden cooperación técnica entre ellos. Cabe recalcar, que CSIRT es manejado por especialistas en ciberseguridad y plantean los proyectos de análisis para la cooperación e iniciativas de política pública.

En Costa Rica, parte de los desafíos de control sobre la ciberseguridad abarca el rol del MICITT y del CSIRT; además de la situación de sensibilización de la población y medidas educativas especializadas en el tema. El país no cuenta con una administración real de la operación y procesos de ciberseguridad, ya que únicamente 4 ingenieros trabajan con todo el aparato estatal. Además, las alianzas público – privadas son incipientes, ocasionando en algunas ocasiones problemáticas de comunicación de vulnerabilidades e incluso de ataques en tiempo real. Es conocido que el sector financiero es uno de los más propensos a ser atacados, sin embargo, los protocolos que los bancos manejan no son claros para las gerencias operativos. Inclusive se puede comentar de ciberataques directos a instituciones como la CCSS o la Asamblea Legislativa.

El aporte económico y educativo en la especialización de profesionales del sector coincide con lo anterior. El esfuerzo de las entidades educativas por exhortar la sensibilización en el uso y protección de datos; la cantidad de opciones en el mercado de educación superior y el presupuesto que se le otorga al MICITT para cubrir las necesidades presentan un desequilibrio. Aunado a que la gran mayoría de profesionales en el país trabajan en el sector privado y que existe una deficiencia de especialistas a nivel global repara un escenario preocupante para lograr ahondar en la necesidad de seguridad cibernética y la efectividad de contener amenazas.

4.3 Estado de la gobernabilidad en Costa Rica: Legislación de las Tecnologías de la Información

La legislación es dinámica, se toma en cuenta el camino recorrido de otros Estados y entidades interestatales para comprender el contexto internacional. Al mismo tiempo, la normativa debe considerar la actualidad costarricense y su proceso de crecimiento como sociedad. Es por ello que la revisión de las condiciones normativas

referentes a las Tecnologías de la Información y su protocolo de seguridad son relevantes en la gobernabilidad y subsecuente gobernanza del país. Tanto la creación de las políticas públicas como el diseño de un marco normativo pretende esclarecer las conductas punibles de los cibercrímenes. De igual forma, el desarrollo estructural y social del país debe ser claro mediante el marco jurídico.

Para lograr identificar la legislación de las TIC's y la ciberseguridad en Costa Rica, se realizó una entrevista sobre el contexto jurídico interestatal y la legislación nacional. Se escanearon posibles mejoras al marco jurídico de la seguridad cibernética y al futuro de las propuestas en la región. La entrevista se realizó a un experto en ciencias forenses con conocimientos técnicos en la actual legislación costarricense. A su vez, se realizó una revisión bibliográfica para complementar los datos obtenidos mediante la entrevista, donde se amplía el alcance del marco normativo y su relevancia en ampliación de instrumentos que le ayudan al ciudadano a protegerse a nivel cibernético.

Las TIC's son responsables por el manejo y control de gran cantidad de servicios que han generado una dependencia con la tecnología, esto los hace vulnerables a los ciberataques a infraestructuras críticas. Con el desarrollo de las TIC's nuevas formas de crimen han surgido, y así, nuevas metodologías para investigar los cibercrímenes están en constante creación. Estos avances han permitido la expansión de las habilidades jurídicas e investigativas de las instituciones gubernamentales encargadas.

Los cambios estatales al aplicar el uso de las TIC's han generado reformas a las políticas públicas en aras de fomentar la digitalización, transparencia y la rendición de cuentas. Costa Rica no ha sido la excepción a este proceso político y social, y la Estrategia Nacional de Ciberseguridad es donde se presenta la relevancia del marco jurídico para la regulación de la seguridad cibernética. En general, en América Latina se puede encontrar una variedad de organismos, normativas y políticas públicas que se tienden a enfocar en avances en el área financiera por ejemplo la Ley de Certificados, Firmas Digitales y Documentos Electrónicos, dejando de lado la regulación de los delitos informáticos y con una carencia severa en la legislación penal referente a la recopilación y análisis de pruebas de medios electrónicos.

Para Costa Rica, previo al diseño de la Estrategia Nacional de Ciberseguridad en 2017, la Ley de Delitos Informáticos del 2012, representa el antecedente más relevante alrededor de la seguridad de los datos cibernéticos, justamente por lo mencionado con anterioridad. Se marca un precedente regional sobre la normativa y sus posibilidades en la región. En esta Ley, se detalla la clasificación de los delitos y se introduce en el Código Penal. Con ella, se le concede un marco de trabajo a la Sección de Delitos Informáticos del Poder Judicial ocasionando un impulso en cuanto al procesamiento de evidencia digital.

El conjunto jurídico que ampara la relación de las TIC's con la ciberseguridad, en el país es considerado pionero en la región puesto que el mismo permite generar transparencia, seguridad jurídica, neutralidad tecnológica y la formación del recurso humano en el área de las TIC's. Sin embargo, se critica la preparación de los fiscales y jueces, ya que no todos tienen la capacidad de preparar y manejar la evidencia procesada por el laboratorio ocasionando una diferencia en el uso de los procesos reactivos de la ciberseguridad.

El panorama del sector de las telecomunicaciones se ha ido ambientando a las necesidades regionales y estatales. Se han manejado conjuntos de políticas que se enfoquen en la disponibilidad de los servicios, penetración de la banda ancha y acceso al ciberespacio, digitalización por medio de los servicios móviles. Sobre estas decisiones imperan las estadísticas: aun con estos esfuerzos existe una división en el acceso a Internet mayoritariamente por rezagos en zonas de bajo desarrollo e ingresos y falta de infraestructura que permita "conectarse" con las comunidades. La multiplicidad de acuerdos en América Latina evidencia la importancia de la inversión e infraestructura necesaria para presentar servicios de calidad que atañen al sector público y privado.

En Costa Rica, esta ruta se ha mantenido de acuerdo con la creación de instrumentos consignados en la Ley General de Telecomunicaciones y la Ley de Fortalecimiento y Modernización de las Entidades Públicas del Sector Telecomunicaciones, mencionadas en la Estrategia Nacional de Ciberseguridad. Estos instrumentos proporcionan el espacio para el desarrollo de las TIC's en el país que

supone la creación de nuevos proyectos basados en uso de recursos, mejora de la normativa, sensibilización de la población y creación de capacidades para los funcionarios de las instituciones públicas.

Sin embargo, la ampliación de la infraestructura y mantenimiento de esta se ha visto afectada por las regulaciones de las instituciones a cargo como el MICITT, el MINAE o el Ministerio de Hacienda. En algunos casos la problemática administrativa del gobierno ha disminuido los presupuestos de las entidades, desintegrando proyectos que tenían el potencial de ampliar la red de TIC's o disminuyendo el presupuesto asignado para tal labor. Como generalidad, el marco normativo dispuesto tanto en la ENCS como fuera de la misma, establece la regulación de la tramitación, los procedimientos y los requisitos para el uso y el potencial impacto de las TIC's pero al mismo tiempo se han descrito desafíos en la progresividad de las políticas públicas que impulsen la infraestructura en el país.

Como se menciona anteriormente, con la Ley de Delitos Informáticos y otras, se expone una reforma relativa a la digitalización y los derechos de la personalidad virtual entre el 2012 y el 2013. La experta consultada indica que los cambios y modificaciones se van generando, tanto a nivel técnico como legal, conforme los cambios sociales lo ameriten. El auge y enfoque en temas de ciberseguridad, que corresponde al MICITT, en el planteamiento de las políticas y proyectos es fundamental para garantizar protección al individuo en el ciberespacio.

Desde el 2001, se han creado las tipologías penales relacionadas con delitos informáticos, pero la normativa no lograba llevar a la regulación de conductas ilícitas. La experta consultada aclara que la legislación y calificaciones han ido progresando y mejorando debido a las experiencias de otras latitudes y esto ha permitido, gracias a la globalización, crear alianzas en sectores de informática, forense y legal. Estas experiencias se traducen en proyección de normativas por parte del MICITT, formación y congresos en temas de ciberseguridad por parte del Colegio de Abogados y mayor comunicación y sensibilización a la población por parte de entidades judiciales como el OIJ.

El reconocimiento penal de los delitos informáticos como lo expone Quirós-Ramírez (2019) *"contiene un gran avance e innovación al incorporar delitos como el de suplantación de identidad"* ya que plantea la sanción cuando una persona toma la identidad de otra en términos cibernéticos, ya sea en redes sociales, páginas web u otros. Además, la mejora en la interpretación de la ley facilita la tarea en situaciones de juicio. Es imperativo mencionar la constante capacitación para los fiscales y jueces de nuevo, ya que nuestro sistema jurídico en ocasiones contiene normativa suficiente pero no autoridades que interpreten y manejen adecuadamente los casos.

Otra parte de la normativa relacionada a seguridad cibernética, uso de la información y transmisión mediante medios informáticos o redes sociales corresponde a la protección de datos personales de los habitantes, el secreto de las comunicaciones y al secreto bancario. También, el Habeas Data como instrumento utilizado en la Sala Constitucional indica los derechos y obligaciones de los habitantes sobre el tratamiento de los datos personales. La normativa en la temática se diseña en el 2011, con la Ley de Protección de la Persona contra el Tratamiento de sus Datos Personales y el principio de Autodeterminación Informativa que garantiza su defensa. La relevancia en el área de ciberseguridad se representa en la ley en tanto la participación ciudadana en el ciberespacio es activa y por ello la información es de uso libre. La concientización en el tratamiento de los datos como privados, ya sea en plataformas de redes sociales o por entidades bancarias, por ejemplo, debe ser autorizada por los individuos. Muchas personas, sin embargo, no tienen el conocimiento del marco jurídico que los protege o de los contratos que se firman a raíz del uso de las plataformas.

El uso indiscriminado de la población hace que el manejo de los datos, inclusive de fotografías o de audios, se puede volver problemático debido a los principios de privacidad de la persona. Por ejemplo, ¿Quién autoriza a un individuo a subir datos de una fiesta? ¿todos los implicados deben tener conocimiento de esta? ¿a quién pertenece la gestión de estos datos? Es por ello, que la utilización de esta información con ligereza podría resultar en una demanda al tener una brecha de conocimiento en la manera que

la normativa se expone para estas situaciones. La educación al individuo no representa un desafío únicamente para Costa Rica, sino a nivel generalizado.

El marco jurídico que comprende las Tecnologías de la Información y la seguridad cibernética tienen un enfoque más maduro en Costa Rica, que, en México, pero, aunque la gobernabilidad esclarece el accionar jurídico, la posición estatal y las políticas públicas a desarrollarse; queda pendiente el análisis de la gobernanza y la forma en que la población y el Sistema intervienen fuera de la normativa, sino en la cotidianeidad.

4.4 Impacto de la ciberseguridad en la gobernanza

La gobernanza está compuesta por diferentes puntos como las acciones gubernamentales, la efectividad del marco jurídico y las políticas públicas. Sin embargo, en el mundo globalizado e interconectado, obviar el peso de las TIC's y la protección de los datos estatales y ciudadanos comprende en un sesgo para el análisis de la gobernanza. La responsabilidad de los Estados responde directamente a las demandas sociales y en el contexto actual esto implica priorizar la tecnología como parte de la vida diaria.

Para lograr generar un análisis de la gobernanza digital alrededor de la ciberseguridad tomando en cuenta los avances de las TIC's y la protección de las instituciones estatales sobre los datos o la digitalización de los mismos, se realizó una entrevista sobre la visión de la cotidianidad costarricense, tomando en cuenta la perspectiva de la privacidad y el esfuerzo sobre el Gobierno Digital. La entrevista se realizó a un especialista en psicología con énfasis en periodismo de medios digitales con conocimiento en TIC's. A su vez, se realizó una revisión bibliográfica para complementar los datos obtenidos mediante la entrevista, donde se enfatizan los índices internos y externos para la medición de la gobernanza digital de Costa Rica.

Para las comunidades digitales, el sentimiento de pertenencia y la construcción de conocimientos a través de Internet significa un cambio social en el mundo globalizado. La preponderancia de la digitalización en los comportamientos en la mayoría de la población trasciende las fronteras y modifica los comportamientos sociales aceptados.

El uso continuo de las TIC's a través de la historia ha convertido a la tecnología en un acelerador del modelo económico, pues incentiva el crecimiento y además sustituye la necesidad de cercanía para las transacciones. Los Estados han sufrido crisis de gobernanza en parte por el fenómeno de globalización y la lentitud del sistema en modificar comportamientos y este es el mayor desafío de la ciberseguridad: aceptar y modificar la visión estatal para seguir protegiendo tanto los datos institucionales como poblacionales que circulan en el ciberespacio.

Históricamente, los Estados se han concentrado en el desarrollo de la Sociedad Digital y sus procesos operacionales, que sean eficientes para una mayoría poblacional. Ha sido de relevancia la creación de infraestructura, el auge de los dispositivos tecnológicos, la comunicación y masificación de la tecnología como tal sin tener en cuenta las vulnerabilidades y amenazas que los avances de la digitalización presentaban. Los riesgos que la planificación había dejado de lado se desarrollaron en los crímenes del Siglo XXI.

Al mismo tiempo que las organizaciones interestatales y los Estados toman conciencia sobre la relevancia de las TIC's, su utilización como estrategia de masificación de información y sus posibles usos en la defensa de los datos es cuando las políticas públicas y los marcos jurídicos empiezan su transformación. A lo largo de 30 años, la legislación costarricense reconoce, caracteriza y sanciona los delitos informáticos, pero de igual manera la falta de protocolos institucionales claros genera vulnerabilidades en el sistema institucional. Los ataques a la Caja Costarricense del Seguro Social y a diferentes entidades bancarias exponen una deficiencia en la conceptualización de la seguridad cibernética.

La fragmentación de la sociedad y su transición al ciberespacio no solo demuestra un cambio generacional, sino un cambio pivotal en el comportamiento, cultura y en la forma de manejo del Estado. Este es solo uno de los desafíos del Estado moderno, enfrentado a la crisis de gobernanza y la inherente crisis fiscal que progresa en el país. La transformación de la sociedad demuestra con mayor claridad las desigualdades existentes en la población, y estas a pesar de la creación de una cibercultura dentro de

las comunidades digitales se llegan a presentar como un espacio flexible y libre que continúa viéndose traducida en el Sistema Internacional como una jerarquización social definida mediante un privilegio de clase.

La brecha social y digital se debe de entender en dos ámbitos, a nivel interestatal, pues existen variaciones en la madurez, apropiación y desarrollo de las TIC's y la ciberseguridad que le permiten al Estado presentar un nivel de gobernanza digital más ampliado. Dirigido por estrategias integrales entre el gobierno y el ejército. O la desigualdad imperante en un territorio, donde existen diferencias entre los grupos sociales o entidades estatales y la seguridad cibernética no esta tan desarrollada y alojada en la formación de los ciudadanos. A continuación, un cuadro resumido del acceso de TIC's en Costa Rica.

Cuadro 4. Acceso y uso de las TIC en el Estado y en los hogares de Costa Rica.

	Estado*	**Hogares**
Generalidades	Conceptualización de e-Gobierno Transformación requiere de políticas de atención a largo plazo que quedan rezagadas debido a los procesos y trámites burocráticos. Existen rezagos principalmente en el sector municipal con respecto a otras instituciones públicas.	Las personas reconocen impacto en todas las áreas de la vida cotidiana de las TIC's: social, educativo, económico, político, laboral. Necesidad para la toma de decisiones de los distintos actores de la sociedad y la creación de políticas públicas eficaces que continúen el desarrollo de la Sociedad Digital.
Contexto Internacional	- Índice de desarrollo e-Gobierno (ONU): América: 0,59 con menor variabilidad entre las notas de los distintos países. Costa Rica con EDGI alto (0,70) superado por Uruguay, Chile, Argentina y Brasil. - Índice de e-Participación - relación gobierno y ciudadanía: 0,76 sim embargo presenta variaciones desde 2008 hasta el 2018.	- Subscripciones telefonía celular: 7,3 M - Personas utilizando Internet: 3900 M - Acceso a Internet de los hogares: 60% - Costo de la canasta de telefonía móvil – puesto 21: 0,45% del ingreso bruto per cápita (IBPC)

	Barómetro de Datos Abiertos: Rezagado – Nota: 31.	- Canasta de internet móvil prepago – puesto 62 – 0,84% IBPC - Canasta de banda ancha fija – puesto 66 – 1,88% IBPC - Reposte de asequibilidad: puesto 4, nota ADI: 76,21
Datos para Costa Rica	- Índice de Transparencia del Sector Público Costarricense (ITSP) - gobierno abierto y datos disponibles en la Web. General: 46,21 de la línea base. 34,55 en todas las entidades. - Índice de Experiencia Pública Digital (IEPD) 2017 – experiencia del usuario y capacidad de realizar trámites en la Web. Sitios web promedio: 46,59. Sin embargo 29 instituciones no poseen página web.	- Telefonía fija:747 mil suscriptores - Telefonía móvil: 8,8 M de suscriptores – aumento del 6% - Internet Fijo: 15/100 habitantes – 744 mil suscripciones – aumento 16,9% - Internet móvil: 4,7 M suscripciones – aumento de 10,4% - Otras estadísticas: Acceso entre los habitantes de telefonía fija: 42% Región Central vs 14-18% resto del país 94% posee un teléfono móvil, 87% un teléfono inteligente. 81% accesa a Internet por medio del celular Internet fijo: ¼ no tiene debido a telefonía móvil, ¼ no lo adquiere por el costo. Acceso a través del celular 98%, computador portátil 39% y computador de escritorio 17%, tabletas o televisor inteligente (15%) - Encuesta Nacional de Hogares (ENAHO): 40,3% de los hogares tiene computadora portátil y 15,1% tiene computador de escritorio, Mas del 50% no cuentan con una computadora - Analfabetismo digital: 45%

Fuente: Elaboración propia con base en el Informe hacia la Sociedad de la Información y el Conocimiento (2019). *Todos los datos de medición del 2018.

A nivel general, el estado costarricense ha experimentado avances en la medición del acceso de los datos y las TIC's. Desde los índices internacionales, se puede identificar que la participación y la comunicación entre el gobierno y los ciudadanos ha sido un desafío. Costa Rica se ha identificado como un país que al menos en los últimos 5 años ha tenido poco o nada de progreso en la relación con la sociedad.

Esto representa una brecha en la gobernanza digital y las iniciativas de protección de datos de manera explícita, pues denota una debilidad en el crecimiento del país en esta área. La situación que enfrenta el gobierno fuera del ámbito virtual, y la crisis de ingobernabilidad latente del país, se traduce directamente a una falta de impulso de nuevas iniciativas que trabajen de forma coordinada con las entidades estatales, especialmente con el MICITT y el CSIRT.

En cuanto a la transparencia del gobierno abierto, los esfuerzos por dar acceso a la información y rendición de cuentas presenta aumentos generales. Se observa que entre las instituciones del Estado hay algunas especialmente rezagadas. El panorama ejemplifica una brecha en el acceso directamente entre las entidades con mejores calificaciones (como los poderes de la Republica y órganos adscritos) y con las peores (sector municipal), así como se presume una falta de presupuesto e interés por aumentar el nivel tecnológico debido a otras situaciones que son priorizadas en la toma de decisiones. La variación en el progreso demuestra que los esfuerzos de mejora de los organismos estatales han disminuido hasta 6 puntos en el Índice.

Con referencia a la experiencia del usuario, el IEPD arroja similitudes con el ITSP. Los datos indican una brecha con los gobiernos locales, puesto que 24 de las municipalidades no tienen una página web para impulsar la transparencia y rendición de cuentas. De igual manera se denota un retraso en la calificación de protección o seguridad de la información y desempeño de los sitios web. La voluntad política tiene una influencia directa en cualquier salto cualitativo de mejora ya sea de información o de

experiencia para los usuarios, y esto a su vez se traduce en seguridad para los ciudadanos sobre el uso y la ciberseguridad del Estado.

En los hogares costarricenses se ha evidenciado un cambio en el panorama de las TIC's, mientras que la telefonía fija y la telefonía móvil revolucionaron las formas de comunicación de la sociedad se encuentra que la necesidad de telefonía fija disminuye frente a la versatilidad de un celular, costo, conectividad a Internet y flexibilidad para realizar otras actividades hace que las personas recurran a tener hasta 1,7 suscripciones. La dinamización del mercado de telefonía es posible debido a la posición privilegiada del país en cuanto a estructura y competencia de los operadores de telecomunicaciones. Siendo el país en los índices mundiales de los más asequibles de la región.

En el plano del ciberespacio e Internet, la situación estatal varia. El costo de Internet fijo de calidad incrementa debido a la posición de desarrollo frente a países como Estados Unidos. La disparidad para obtener los servicios evidencia un desuso frente a la conectividad móvil o el costo más allá del presupuesto por hogar para los servicios esenciales. Internet es utilizado mayoritariamente con carácter social mediante las plataformas como Facebook, ver videos o imágenes o recibir y enviar correos electrónicos. Por otro lado, la tenencia de Internet fijo indica una brecha por grupo etario donde los más jóvenes tienen mayor acceso tanto a la conectividad como a los dispositivos tipo smartphone evidenciando que las personas mayores de 55 años tienen más dificultades para mantenerse al corriente con los avances en las TIC's.

De acuerdo con la ENAHO, la brecha digital se concentra en el analfabetismo digital y el costo elevado en comparación al estilo de vida en ciertas áreas geográficas del país. Los hogares desconectados argumentan que no necesitan de conectividad a Internet o que a pesar de tener dispositivos que tienen acceso al ciberespacio, no saben que hacer o como utilizarlo. El 45% de los hogares sin conexión requieren de una iniciativa pública que cubra las necesidades de sensibilización y educación de la población de una forma inclusiva. Parte de los problemas identificados también se debe a la cobertura de la infraestructura para poder conectar a los hogares en zonas rurales de difícil acceso.

La exclusión de este sector de la población genera desigualdad social, asociada con la gobernanza del mundo digital y el acceso a las TIC's. Plantea una brecha en cuanto a la educación alrededor de la protección de los datos personales y estatales, puesto que la población no entiende los peligros y vulnerabilidades asociados a las prácticas de uso. El experto consultado agrega que las entidades públicas tienen un manejo precario del tema de privacidad y seguridad de la información que resguardan. La Contraloría General de la Republica ha señalado esto con la información sensible del Ministerio de Hacienda o de la CCSS. Se indica que es por esta actitud relajada hacia las políticas públicas es que los ciudadanos desconocen el impacto de los términos de privacidad de las plataformas que utilizan.

Adicional a la situación social, se debe entender que los ejecutores de las políticas alrededor de la ciberseguridad se componen de un grupo de personas especializadas. En el caso de Costa Rica, el recurso humano que posee esta especialización es limitada, si bien las instituciones de educación superior tienen una oferta sobre ciberseguridad, la mayoría de los ingenieros terminan concentrándose en el sector privado. La diferencia con las instituciones estatales deja en peligro la administración y el manejo de la ciberseguridad en manos de 4 personas del CSIRT para todo el país.

Como se menciona anteriormente, la falta de capacitación inclusive representa un desafío en la investigación y manejo jurídico de los casos con pruebas electrónicas. Esta deficiencia es aún más evidente en el cumplimiento de protocolos de seguridad, mientras que la brecha interinstitucional se agrava entre el gobierno central y los gobiernos locales. La falta de voluntad política para atraer a mayor cantidad de profesionales representa un serio problema de innovación, cumplimiento y rendimiento eficaz de la ciberseguridad.

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

El presente capitulo expone los argumentos finales de la investigación. Se presentan los argumentos principales sobre el análisis bibliográfico y de las síntesis de las entrevistas como parte de la exploración cualitativa alrededor de las tecnologías de la información y de la ciberseguridad. Lo que representa un impacto en la sociedad global y su enfoque a lo largo del tiempo en la innovación frente a la protección de los derechos fundamentales en el ciberespacio.

Al detallar las razones que indican el nivel de gobernanza y ciberseguridad sobre el cual está trabajando Costa Rica en la actualidad. Se pueden observar beneficios y mejoras en el sistema nacional de manejo del sector, dando un recorrido histórico y caracterizando la necesidad de Estrategias de Ciberseguridad para el avance de las tecnologías de la información en las comunidades virtuales. En reconocimiento de la importancia de este nuevo actor en las relaciones internacionales predispone el uso de herramientas que fomenten el conocimiento y el manejo de la cooperación digital.

Asimismo, se plantea la estructuración de la gobernanza frente a dos ejes que interconectan al aparato estatal, las instituciones y los ciudadanos, y la crisis traducida al mundo virtual. La forma de operación sobre la estructura institucional imperante revela los desafíos hacia una mejor política pública de tecnología y seguridad cibernética, mientras que el impacto en la ciudadanía representa la oportunidad de mejorar la inclusión digital en el país.

A continuación, se presentan una serie de conclusiones de la investigación que reflejan la interconectividad de las TIC y la ciberseguridad desde el ámbito histórico, jurídico, de la experiencia de otros países y finalmente de la situación de Costa Rica. Además, se plantean recomendaciones para diferentes actores del Sistema Internacional que representan progreso hacia mejor calidad de ciberseguridad para los costarricenses.

5.1 Conclusiones

El fenómeno de globalización ha sido trascendental en la acogida del ciberespacio por la sociedad. Los cambios en el comportamiento comunitario han demostrado que los individuos ven como parte de la cotidianeidad los usos de las tecnologías de la información y que la penetración de estos llega prácticamente a todos los espacios geográficos, así como a la salud, economía, cultura, etc.

Inicialmente, el reconocimiento de la evolución en los avances tecnológicos ha simplificado la vida para las personas y forzado a los Estados a flexibilizarse dando acogida a la tecnología y la digitalización de los procesos operacionales de las instituciones públicas. Estas iniciativas han sido ampliamente discutidas por los gobiernos, y la madurez en la compresión del uso de las TIC's varia de país a país. De manera paralela a este punto de desarrollo, la liquidez en las comunidades virtuales abre oportunidades para que las opciones delictivas crezcan en el ciberespacio. La fragmentación e individualización que ha visto la evolución de las tecnologías de la Información ha llevado a algunas personas o grupos a organizarse para cometer los crímenes tecnológicos del Siglo XXI.

El modelo económico y político ha permitido el acceso del Internet convirtiéndolo en una de las herramientas más utilizadas para diferentes ámbitos de la vida en sociedad y permitiendo la colaboración con agilidad entre los Estados. Desde la invención del computador para avances en la física aplicada hasta las variaciones a los costos de consumo de dispositivos móviles, la economía se encuentra incentivando al sector tecnológico para continuar innovando, y de manera primaria este fue el plan global sobre el uso de la Web. Pero la búsqueda del poder ha sido parte indispensable del juego económico y político y este sigue siendo el escenario en el ciberespacio.

Sin embargo, la ampliación en el uso del ciberespacio genera iniciativas militares como la Deep Web, que fracasan en la construcción operacional sobre el manejo de Internet. La DW pone a disposición de aquellos que lideran los actos ilícitos para el tráfico de armas, personas, drogas, entre otros. Es por ello, que la tipología de los cibercrímenes

es tan extensa y variada, no solo para aquellos que sufren de estafas o de acoso, sino como una problemática más general de situaciones ilícitas que son de preocupación para los Estados y organismos internacionales hoy en día. El uso indiscriminado de la DW ha generado inclusive redes de hackers especializados en la corrupción del Sistema Internacional por medio de la incertidumbre que genera la Sociedad del Riesgo.

Al aparecer las comunidades digitales, se instaura un marco regulatorio que es frecuentemente obviado por los cibercriminales en la búsqueda de poder e información. Este tipo de estrategia no pasa desapercibida por los Estados, que al mando del sector militar diseñan estrategias para la Guerra Digital o de la Información. El mercado y los sucesos internacionales se prestan ante estas situaciones creando en el mundo virtual una serie de acciones que logran manipular las noticias, la percepción y el acceso de la información hacia los ciudadanos. Mas aun, se logra accesar a datos que son confidenciales del Estado.

El temor y la desconfianza en las comunidades digitales también ocasionan roces con la crisis de gobernanza en la actualidad. Los ciberdelitos que surgen con mayor complejidad, en muchas ocasiones, son muestras del poder del otro en el mundo virtual. Algo que para los Estados modernos debe ser combatido y aplacado, un nuevo entorno frente a una Guerra Digital con actores que no son tradicionales, y tampoco buscan ventajas de forma tradicional pues la tenencia de información lo es todo en el mundo globalizado.

Por tal razón, el desarrollo de las estrategias nacionales de ciberseguridad se vuelve relevantes hacia las vulnerabilidades de los crímenes del Siglo XXI. Con un claro corte militar, estas inician con las formas más comunes de ciberdelitos y su análisis. El surgimiento de estos actores del ciberespacio también sugiere que debe incrementarse el manejo y conocimiento de los alcances de los Estados en este nuevo territorio. Plantear desde las ENCS la cooperación y la regulación de las TIC’s, la infraestructura y el reconocimiento de los riesgos en los países con mayor desarrollo se vuelve una posibilidad.

Algunos Estados comprenden la necesidad de ahondar sobre el tema de seguridad; algunos se encuentran rezagados en la materia. Es por ello por lo que los enfoques alrededor del ciberespacio pueden llegar a variar, debido a presupuesto, importancia en las agendas políticas estatales, infraestructura o especializaciones. Lo relevante se muestra en varios ejes temáticos de acción de la ciberseguridad:

1. La necesidad de cooperación: Proteger el ciberespacio no se puede observar como el rol de un solo actor, no puede tratarse como el control de lo rigidez física y esto es algo que los Estados están flexibilizando.
2. La importancia de los nuevos especialistas en estrategia virtual se vuelve imperativo para la gobernanza digital
3. El rol estatal en la educación alrededor de las TIC's, su impacto y su penetración, es igual de importante que la digitalización del Estado.

La ENCS estadounidense representa una versión simple pero clara con respecto a la innovación tecnológica, su posición frente a la gobernanza digital, la protección de datos y la necesidad de un marco global de cooperación liderado por el país. Hay que tener presente que Estados Unidos es una potencia mundial, y su economía depende en la actualidad de las transacciones comerciales ayudadas por Internet y el ciberespacio por lo que mantenerse en los primeros lugares en ciberseguridad es necesario para salvaguardar la información estatal y la protección de las empresas privadas.

En el caso de Estados Unidos, debido a su política comercial es que la penetración de las TIC's se toma como una realidad. Sin embargo, los beneficios más allá de lo económico son parcializados para los ciudadanos. Hay que tener en cuenta que, aunque se presente como potencia económica, la desigualdad social y la brecha digital existe en este país. La protección de la infraestructura critica, el aumento de los servicios tecnológicos y la protección de datos para los ciudadanos consolidan la estrategia de la ciberseguridad como pivote para estandarizar practicas frente a conjuntos de países u organismos internacionales. Estados Unidos continúa representando las tendencias en el continente más seguras y es debido a sus socios comerciales en el sector privado,

pues a nivel de gobernanza no se ahonda si existe comunicación y transparencia entre el gobierno federal y la ciudadanía.

En cambio, como se ha mencionado anteriormente la historia para América Latina es distinta, no solo por la visión más contemporánea sobre la protección de datos, una visión más humanista. Sino también por el hecho que las ENCS y la priorización de los gobiernos no presenta aun una planificación madura, dejando vulnerable a la región frente a posibles ciberataques. Los esfuerzos por la creación de la red CSIRT-CERT, la organización de políticas públicas que incentiven la seguridad cibernética y la penetración de las TIC's por parte de la CEPAL y el BID son muestras de la realidad: la desigualdad impera en la región.

En los casos de estudio, México y Costa Rica, se vislumbra una diferencia si acaso de un par de años de observación y desarrollo de políticas públicas para el desarrollo de la ciberseguridad. Costa Rica hasta el cambio progresivo de la legislación a partir del 2011 no era considerado tampoco como país con un fuerte sistema de protección. Por su parte, el Estado mexicano se encuentra en la realización incipiente de legislación y organismo que regulen y administren a nivel interno las amenazas y vulnerabilidades.

Por tanto, al identificar el estado de la gobernabilidad de la ciberseguridad, uno de los problemas que intentan solventar las ENCS se refiere directamente a la detección de riesgos, amenazas y vulnerabilidades que afecten a las entidades estatales y al sector privado, pero sin un marco normativo o las instituciones que logren aplicar el marco de manera eficiente es una realidad que los ataques en la mayoría de los casos pasarían desapercibidos. Las pérdidas económicas cuantificadas fácilmente representan un detrimento en el crecimiento económico de cualquier país. Es por ello que tanto México como Costa Rica se han esforzado por mejorar su defensa ante los ciber crímenes.

En muchos países de la región se ha observado la voluntad política por hacer realidad las estrategias de ciberseguridad y establecer las mediciones correspondientes para demostrar un avance a nivel de las tecnologías de la información que genere un impacto en el resguardo de datos. En Costa Rica, la ENCS cubre la necesidad de

cooperación nacional, la sensibilización hacia la seguridad cibernética como deber de los usuarios de TIC's, revisión del marco jurídico, protección a la infraestructura crítica y cooperación internacional.

En cuanto a la cooperación nacional, los actores del sistema costarricense deben tener la voluntad política para colaborar con la estrategia que coordine la colaboración y el intercambio cuando exista una acción contra la seguridad cibernética nacional. El MICITT es la entidad encargada de la eficiencia de la implementación de estos protocolos, sin embargo, no se tiene predispuesto la necesidad de ampliar el departamento del CSIRT para poder manejar más de 300 instituciones del Estado.

Asegurar el entendimiento de la población sobre las medidas que fomenten la seguridad cibernética conlleva un planeamiento sectorial. El nivel de información que se le da a los funcionarios de las instituciones públicas, a las empresas del sector privado van a variar frente a contenido explicado para la población general. La necesidad que el Estado tenga una conciencia sobre la necesidad de la ciberseguridad, el apoyo que se le debe dar a las TIC's y la puesta en marcha de buenas prácticas de uso del Internet son imprescindible para alcanzar a un cambio en la percepción ciudadana sobre los cuidados o riesgos de acciones mínimas como transferencias bancarias o publicar fotografías en redes sociales. El fomento de la ciberresiliencia como nación permite disminuir un sector de la brecha digital dirigida en el conocimiento de las herramientas tecnológicas.

La infraestructura crítica permite el funcionamiento de los servicios gubernamentales y en muchas ocasiones del sector privado, son parte de los servicios esenciales que de verse afectados ocasionan efectos negativos en el bienestar social y económico. El impulso en la ENCS de diseñar propuestas de políticas públicas pensando en esto, asegura que la funcionalidad y las operaciones mantengan un estándar de calidad apropiado y que se pueda mitigar o restaurar con mayor facilidad un sistema de redes (servidores) con agilidad en caso de un ciberataque.

A pesar de que la estrategia indica la creación de directrices para la protección de la infraestructura crítica y alianzas entre los operadores y el Estado deja de lado que la concentración de estas es mayoritaria en la Región Central del país, que a su vez focaliza las instituciones que son usualmente perpetradas por cibercriminales. El faltante de especialistas también hace complejo el manejo adecuado de infraestructura, pues hay una deficiencia de expertos en el sector público que aclaren dudas y trabajen de forma adecuada protocolos de protección.

La falta de especialistas posee un impacto directo a su vez con la gestión de los riesgos y amenazas. Muchas entidades son evaluadas por los servicios que proveen en línea, pero no se toma en cuenta en qué medida las operaciones se ven afectadas por ataques cibernéticos o los procesos de gestión para la ciberresiliencia que el juego político permite exponer a la institución. Lugares como el OIJ o algunas municipalidades ofrecen variedad de servicios en línea que sin duda alguna carece de mediciones concretas para garantizar la seguridad y transparencia al usuario.

La cooperación internacional se expande hacia la ciberseguridad con diálogos interestatales y con organismos internacionales que fomenten el desarrollo y la colaboración en diferentes ámbitos como la educación o en lo jurídico (penal y forense). La ENCS se dio a raíz de esfuerzos con la OEA y fomentar la comunicación de experiencias en foros especializados, crea oportunidades de crecimiento local y para movilizar los recursos en un ambiente dinámico como lo es la tecnología.

Con respecto a la legislación, Costa Rica ha presentado avances en cuanto a la cantidad de normativa que ayude con la regulación y la gobernabilidad de las tecnologías de la información. Sin embargo, los procesos operacionales ocasionan en algunos casos confusión sobre los alcances de la misma, por ejemplo, los estudios de factibilidad para construir infraestructura de telecomunicaciones en áreas poco accesibles o la falta de procesos para la recolección de datos sensibles de la población.

El aumento del marco jurídico a partir de los cambios entre el 2011 y el 2013, inclusive dentro del Código Penal, indicaban la voluntad política del gobierno por

interponer mejoras que llegaran a tener un efecto positivo en las instituciones y la población. Sin embargo, los avances investigados posteriormente no indican mayores cambios a las definiciones de ciberseguridad. Esto representa una situación precaria ante el dinamismo de los ciber atacantes y la rápida evolución de cibercrímenes. Los expertos consultados hablan de mayor preparación de los especialistas que manejan el área, pero cuando se indaga sobre la normativa, como todo proceso gubernamental debe modificarse basado en la experiencia de otros países y la necesidad interna.

Es difícil conciliar que la responsabilidad recaiga primariamente frente al MICITT, la PRODHAB, y el CSIRT como entes reguladores de política pública a los sucesos delictivos en el ciberespacio. Mientras que al Poder Judicial simplemente como ejecutores. Las instituciones no pueden elaborar de forma eficiente protocolos reales para los sectores del gobierno, puesto que no cuentan con los recursos adecuados ni con el recurso humano para el desarrollo. Casos concretos representan el llamado caso UPAD y la vulneración al BCR. En este plano, solo queda agregar el desequilibrio frente al sector privado y el limitado poder que tiene el tema frente a las distintas crisis que afronta el Estado costarricense.

Es de entender, que cantidad de leyes no resulta en calidad o transparencia para la ciudadanía. Las iniciativas para el desarrollo de telecomunicaciones y ciberseguridad no forman parte de la agenda política del Legislativo. Es por ello que una limitación al presupuesto para campañas de sensibilización a la población o para la contratación de especialistas en la digitalización y protección de datos para el gobierno se ha visto limitada. Los riesgos ante esto se traducen directamente en pérdidas económicas y porque no inclusive en atracción a inversión ante la falta de soporte frente a posibles ataques.

Por otro lado, el enfoque de las leyes que Costa Rica tiene es innovadoras en la región. La madurez de la ENCS, la política de los gobiernos y los esfuerzos por proteger el Estado, como se menciona, varia. Haciendo posible la cooperación regional y abrir los canales de comunicación para mantener un estándar mínimo de la ciberseguridad. El hecho que el país exhiba mejores condiciones se traduce a una imagen positiva en la

importancia de la tecnología, a pesar de los potenciales riesgos al detallar los desafíos. Es una trayectoria que a largo plazo debe ser tomada en cuenta y cuyo manejo diplomático va a incidir en planes de trabajo para dinamizar el actuar del sector a nivel interno y externo.

Al analizar el tema de gobernabilidad y gobernanza en el contexto digital conlleva a utilizar la terminología de forma complementaria, no intercambiable. La gobernabilidad comprende el marco jurídico, que anteriormente fue expuesto. Mientras que la gobernanza toma en cuenta factores sociales, económicos, jurídicos y tecnológicos que permiten describir el impacto en la sociedad costarricense. La gobernanza digital no comprende exclusivamente la ciberseguridad, y es por ello que explica la razón por la cual el tema cobra relevancia investigativa.

Las TIC’s han cambiado la perspectiva sobre el manejo del Estado y el rol de la sociedad. Incidentalmente, el acceso a tecnología ha evidenciado la desigualdad en un nivel más de la población. Aunado a esto, el desarrollo local y autónomo al gobierno central es parte de la desigualdad estatal. A mayor acceso, educación y uso de las TIC se expande la amenaza de afrontar un ciberataque; pero a más desconocimiento sobre los riesgos sistemáticos mayor posibilidad de ser el ente vulnerado.

¿Qué implica lo anterior? Que un individuo con estudios universitarios y un dispositivo inteligente, tiene mayores posibilidades de ser objeto de algún tipo de ciberataque, pero con el conocimiento de reconocerlo y reportarlo. Mientras que un adulto mayor, con limitaciones tecnológicas, va a ser víctima con mayor facilidad de un ataque como phishing a su correo electrónico, o seguir las instrucciones de una llamada para estafarle.

Estas diferencias hacen que la gobernanza digital sea un tema muy amplio y que la ciberseguridad también lo sea. Si se toma en cuenta solo a la ciudadanía, el Estado debe garantizar:

1. Que se están protegiendo los datos de la nube que pertenecen al Estado. Los datos sensibles de la CCSS, del Ministerio de Hacienda o del Banco Central deberían tener los protocolos más claros y transparentes ante posibles ataques.
2. La educación y sensibilización inclusiva y sectorizada para la población, desde campañas publicitarias hasta cursos e incursión comunitaria para que todas las personas tengan conocimientos básicos sobre ataques.
3. No se están utilizando o resguardando datos sensibles para uso propio del gobierno, cuando un caso no esté siendo investigado.

Mientras que, al comparar, la gobernanza y transparencia de las instituciones en la rendición de cuentas; se puede notar que:

1. La disparidad entre el gobierno central y sus instituciones con los gobiernos locales expone al central a manejar planes e infraestructura robusta y monitoreada que exponga ciberataques.
2. La infraestructura critica del Estado debe ser administrada de manera eficiente y clara para la población. Los planes de mantener la tecnología y la seguridad deben ser dinámicos, y al corriente de las tendencias.
3. Todos los funcionarios del gobierno deberían entender y mantener los estándares de calidad frente a las practicas propias de la ciberseguridad.
4. La voluntad de los gobernantes ha de exponer los riesgos de incumplimiento de las políticas públicas que sean progresivas ante los avances globales.
5. La cooperación intersectorial debe ser inclusiva, y coadyubada por la digitalización del Estado permitiendo comunicación en tiempo real, priorización de vulnerabilidades y reconocimiento de ciberataques.

Ante lo expuesto, cabe recalcar que el impacto de la ciberseguridad en la gobernanza de Costa Rica debe ser parte del proyecto país. La inclusividad de la población, como actor en la regulación del ciberespacio permite la ejecución transparente de las leyes y las políticas públicas. El esfuerzo estatal por su parte debe de ser constante para mejorar la atención al ciudadano, la digitalización para mejorar la eficacia del aparato estatal y la seguridad para su protección. La voluntad política es en gran parte

el mayor desafío para la gobernanza y ciberseguridad, sin embargo, la relevancia del tema ha permitido la constante observación a los problemas relacionados a la seguridad de los datos.

5.2 Recomendaciones

El tema de ciberseguridad a nivel global es aún novedoso, y como estrategia de seguridad comprende características que han ido progresando para realmente proveer a la población de forma holística la protección de sus datos y al Estado un espacio con mayor complejidad para desarrollarse. A nivel internacional, la seguridad cibernética forma parte del balance del poder de los Estados, de una nueva forma de vivir, y en la actualidad en conjunto con la tecnología, es la nueva realidad. Para Costa Rica esto implica oportunidades de desarrollo, aumento de especialistas y priorización en las agendas políticas en todas las instituciones públicas.

Desde la óptica investigada se generan ciertas sugerencias para estudios posteriores con alcance similar, para los organismos internacionales que requieren crear normas regionales para un mínimo de calidad en las telecomunicaciones y la ciberseguridad, revisión del estado de las entidades reguladoras de la ciberseguridad y un potencial reajuste a las políticas públicas costarricenses.

Los avances tecnológicos y los procesos de digitalización han expandido el marco de trabajo para los países, es por ello que se recomienda a la Organización de Estados Americanos para que coadyuve en la creación de una normativa regional que fomente el progreso en el ámbito de la ciberseguridad como parte de la agenda de los Estados con la finalidad de mantener altos índices de cooperación técnica. Además, que se cree un espacio para diálogos con entidades intersectoriales en aras de una revisión constante de las políticas reguladoras de la ciberseguridad.

En cuanto al desarrollo de canales de colaboren con la gobernabilidad, se indica al Estado costarricenses la búsqueda y relación de cooperación técnica con organismos interestatales para la coordinación de estudios y la ampliación de las iniciativas de protección y regulación de infraestructura critica a todas las entidades estatales. A su

vez, en conjunto con especialistas del sector privado se pueda realizar un estudio de vulnerabilidades y riesgos conforme avance la iniciativa de Gobierno Digital, cuyo objetivo debe garantizar el manejo holístico de la realidad cibernética nacional.

Igualmente, en cuanto a gobernabilidad y visibilidad regional del trabajo del CSIRT se propone al Ministerio de Ciencia, Tecnología y Telecomunicaciones la creación de una iniciativa con presupuesto de las entidades del Gobierno Central para asignar a un especialista en Ciberseguridad en las instituciones para que administren y modernicen los sistemas de protección de datos. Asimismo, estos especialistas estarían bajo el CSIRT en la comunicación permanente de amenazas al Estado o al sector privado.

Con respecto a la agilización de procesos que conllevan a mejor gobernanza digital los gobiernos locales, en conjunto con el MICITT lanzar una iniciativa de inclusión tecnológica tanto para digitalizar la información, creación de páginas de los gobiernos y protección de los datos con el fin de llevar transparencia a la administración, estado y manejo de los recursos locales. Esta propuesta tendría que analizar inclusive el proceso a futuro sobre el mantenimiento de los datos y el uso correcto de la ciberseguridad.

El conjunto de los Ministerios de Tecnología, Educación y Planificación para sobrellevar el alcance de las ENCS y la medición de la gobernanza digital en la sociedad se recomienda organizar una campaña sectorizada de atención a las necesidades de telecomunicación con un rubro sobre ciberseguridad y afectaciones comunes para trabajar en las comunidades más vulnerables del país con el fin de mejorar la calidad y acceso a las TIC’s y la seguridad cibernética.

En cuanto a la especialización y mejora continua de la seguridad nacional y su impacto en la generación de políticas públicas se indica a la Sección de Delitos Informáticos del Poder Judicial en conjunto con la Comisión de Asuntos Jurídicos de la Asamblea Legislativa una revisión de la normativa de los ciberdelitos y el progreso global que se ha hecho en el marco de la Convención de Budapest para que se dinamice la formulación de proyectos e iniciativas derivadas de los avances en ciberseguridad y que logren una mayor flexibilidad en el caso de ciberataques al Estado.

De igual manera, a la Sección de Delitos Informáticos del Poder Judicial para realizar activamente campañas de formación e información a los especialistas encargados de la regulación normativa (jueces y fiscales) sobre las tecnologías de la información y el procesamiento de evidencia para delitos informáticos. Asimismo, en conjunto con el CSIRT mantener un enlace de comunicación constante con el fin de eficiencia en los procesos de identificación de vulnerabilidades.

Por último, en cuanto a futuras investigaciones y para futuros internacionalistas u otra carrera con interés en la ciberseguridad y el impacto en la gobernanza se recomienda ampliar la investigación a las alianzas público – privadas. El impacto en la toma de decisiones de los gobiernos sobre la ciberseguridad. Además de replicar la investigación con la perspectiva privada permite el conocimiento del Estados de todas los sectores y el posible impacto económico para el país.

Bibliografía

Aguilar-Antonio, J.-M. (Diciembre 2019 - Mayo 2019 de 2019). Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad. *URVIO, Revista Latinoamericana de Estudios de Segurida*, 24-40. Recuperado el 22 de Mayo de 2020, de https://revistas.flacsoandes.edu.ec/urvio/issue/view/181/220

Asensi, V. (1993). Evolución histórica de las Tecnologías de la Información y su aplicación en el proceso documental. (E. Complutense, Ed.) *Revista General de Información yDocumentación,, 3*, págs. 131-141. Recuperado el 9 de Mayo de 2020, de https://revistas.ucm.es/index.php/RGID/article/view/RGID9393220131A

Ávila , W. (Enero-Junio de 2013). Hacia una reflexión histórica de las TIC. *Hallazgos, 10*(19), págs. 213-233. Recuperado el 9 de Mayo de 2020, de https://www.redalyc.org/pdf/4138/413835217013.pdf

Bartolomé, M. (2 de Diciembre de 2019). Amenazas y conflictos híbridos: características distintivas, evolución en el tiempo y manifestaciones preponderantes. *URVIO, Revista Latinoamericana de Estudios de Seguridad*, págs. 8-23. Recuperado el 14 de Mayo de 2020, de https://revistas.flacsoandes.edu.ec/urvio/issue/view/181/220

Belloch, C. (2015). *Las Tecnologías de la Información y Comunicación en el aprendizaje.* Valencia: Universidad de Valencia. Recuperado el 10 de Mayo de 2020, de https://www.uv.es/bellochc/pedagogia/EVA1.pdf

Camou, A. (2001). *Los desafíos de la gobernabilidad.* México D.F.: Flacso/IISUNAM/Plaza y Valdés. Recuperado el 27 de Mayo de 2020, de https://issuu.com/jooselitoparker/docs/los_desaf__os_de_la_gobernabilidad

Canaza, F. (1 de Junio de 2018). La sociedad 2.0 y el espejismo de las redes sociales en la modernidad líquida. *In Crescendo, 9*, págs. 221-247. Recuperado el 12 de Mayo de 2020, de https://dialnet.unirioja.es/servlet/articulo?codigo=6853005

Cancino, H. (23 de Enero de 2020). *Martín Sola y el empleo en ciberseguridad: "América Latina es hoy, después de Asia, la zona que más vacantes tiene que llenar.* Recuperado el 3 de Febrero de 2020, de americaeconomia:

https://tecno.americaeconomia.com/articulos/martin-sola-y-el-empleo-en-ciberseguridad-america-latina-es-hoy-despues-de-asia-la-zona

Chacon Jimenez, K. (5 de Abril de 2018). *Conozca la oficina que vela por la ciberseguridad en Costa Rica*. Recuperado el 3 de Febrero de 2020, de El Financiero: https://www.elfinancierocr.com/tecnologia/conozca-la-oficina-que-vela-por-la-ciberseguridad/XK67WOUVPFAYRN3MNPDJSGYHTA/story/

Cid, P., & Perpinyà, R. (2013). *Cómo y dónde buscar fuentes de información.* Bellaterra: Universitat Autònoma de Barcelona. Recuperado el 18 de Febrero de 2020, de https://publicacions.uab.cat/pdf_llibres/MAT0227.pdf

COMEXI. (2018). *Perspectiva de ciberseguridad en México.* México: COMEXI. Recuperado el 10 de Febrero de 2020, de https://consejomexicano.org/multimedia/1528987628-817.pdf

Cundins, E. (Diciembre de 2017). Prepararse ¿para qué guerra? *Visión Conjunta*(17), págs. 3-10. Recuperado el 13 de Mayo de 2020, de http://www.esgcffaa.edu.ar/pdf/ESGCFFAA-2016_pdf-46.pdf

Escobar, R. (Enero-Marzo de 2003). La sociedad del riesgo global. *Revista Espanola de Investigaciones Sociologicas*, págs. 279-303. Recuperado el 13 de Mayo de 2020, de http://www.reis.cis.es/REIS/PDF/REIS_101_131166619689246.pdf

Estado de México. (2017). *Estrategia Nacional de Ciberseguridad.* México: Gobierno del Estado de México. Recuperado el 1 de Febrero de 2020, de https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

Fischer, E. (2016). *Cybersecurity Issues and Challenges: In Brief.* Congressional Research Service. Recuperado el 17 de Mayo de 2020, de https://pdfs.semanticscholar.org/65e3/4c9bb7330fcfec378394b5d308b6a323947d.pdf

Hernández, R., Fernández, C., & Baptista, M. (2014). *Metodología de la Investigación.* México D.F: McGraw-Hill. Recuperado el 15 de Febrero de 2020, de https://www.uca.ac.cr/wp-content/uploads/2017/10/Investigacion.pdf

Johnson, T. (2015). *Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare.* (C. Press, Ed.) Boca Raton, Florida: Taylor & Francis Group. Recuperado el 20 de Febrero de 2020

Korstanje, M. (Enero-Abril de 2010). Reseña de "La sociedad del riesgo: hacia una nueva modernidad" de Beck, Ulrich. *Economía, Sociedad y Territorio*, págs. 275-281. Recuperado el 13 de Mayo de 2020, de https://www.redalyc.org/pdf/111/11112509011.pdf

La Gaceta. (13 de Octubre de 2005). *Ley de Certificados, Firmas Digitales y Documentos Electrónicos.* San José: La Gaceta. Recuperado el 9 de Febrero de 2020, de http://www.firmadigital.go.cr/Documentos/ley%208454.pdf

La Gaceta. (2008). *Ley General de Telecomunicaciones.* San José: La Gaceta. Recuperado el 9 de Febrero de 2020, de http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=63431&nValor3=91176&strTipM=TC

La Gaceta. (2012). *Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal.* San José: La Gaceta. Recuperado el 9 de Febrero de 2020, de http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=73583&nValor3=90354&strTipM=TC

Launay, C. (Diciembre de 2005). La gobernanza: Estado, ciudadanía y renovación de lo político. Origen, definición e. (C. d. (CINEP), Ed.) *Controversia, 185*. Recuperado el 27 de Mayo de 2020, de http://bibliotecavirtual.clacso.org.ar/Colombia/cinep/20100925104922/lagobernanzaCo

Le Texier, T. (2004). *Gouvernances.* Paris: Rhinoceros.

Locatelli, O. (Diciembre de 2017). Arte Operacional: determinación del Centro de Gravedad. *Visión Conjunta*, págs. 40-46. Recuperado el 13 de Mayo de 2020, de http://www.esgcffaa.edu.ar/pdf/ESGCFFAA-2016_pdf-46.pdf

López, J. (21 de Julio de 2009). El concepto de legitimidad en perspectiva histórica. *Cuadernos Electrónicos de Filosofía del Derecho* . Recuperado el 25 de Mayo de 2020, de

https://www.researchgate.net/publication/49941512_El_concepto_de_legitimidad_en_perspectiva_historica

Martínez, L. M., Leyva, M. E., Félix , L. F., Cecenas, P. E., & Ontiveros, V. C. (2014). *Virtualidad, ciberespacio y comunidades virtuales.* México: Red Durango de Investigadores Educativos, A. C. Recuperado el 10 de Mayo de 2020, de http://www.redie.mx/librosyrevistas/libros/vircibercomun.pdf

Ministerio de Ciencia, Tecnología y Telecomunicaciones. (2017). *Estrategia Nacional de Ciberseguridad Costa Rica 2017.* San José, C. R.: MICITT. Recuperado el 1 de Febrero de 2020, de http://www.conicit.go.cr/biblioteca/publicaciones/publica_cyt/Estrategia-Nacional-Ciberseguridad-CR-19-10-17.pdf

Moreno, A., & Suárez, C. (2010). Las comunidades virtuales como nuevas formas de relación social: Elementos para el análisis. *Espéculo: Revista de Estudios Literarios, 43*. Recuperado el 10 de Mayo de 2020, de https://www.biblioteca.org.ar/libros/151845.pdf

Muñoz, M., & Nicaragua, R. (Enero-Julio de 2014). Un acercamiento a la brecha digital en Costa Rica desde el punto de vista del acceso, la conectividad y la alfabetización digital. *E-Ciencias de la Información, 4*. Recuperado el 12 de Mayo de 2020, de https://dialnet.unirioja.es/servlet/articulo?codigo=5689599

Murolo, N. (Noviembre de 2010). Cuatro conceptos para interpretar el cruce entre digitalización y sociedad. *KAIROS. Revista de Temas Sociales.* (26). Recuperado el 11 de Mayo de 2020, de https://dialnet.unirioja.es/servlet/articulo?codigo=3702504

OAS. (2013). *Tendencias en la Seguridad Cibernética en América Latina y el Caribe y Respuestas de los Gobiernos .* Secretaría de Seguridad Multidimensional. Organization of American States. Recuperado el 17 de Mayo de 2020, de https://www.sites.oas.org/cyber/Documents/2013%20-%20Tendencias%20en%20la%20Seguridad%20Cibern%C3%A9tica%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe%20y%20Respuestas%20de%20los%20Gobiernos.pdf

Observatorio de la Ciberseguridad en América Latina y el Caribe. (2016). *Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe? .* Banco Interamericano de Desarrollo . Recuperado el 22 de Mayo de 2020, de https://publications.iadb.org/publications/spanish/document/Ciberseguridad-%C2%BFEstamos-preparados-en-Am%C3%A9rica-Latina-y-el-Caribe.pdf

Padilla, P. (2018). *Surgimiento de un nuevo actor internacional en el Siglo XXI: Influencia de las tecnologías de la información en el Sistema Internacional (2013-2017).* San José: Universidad Internacional de las Americas. Recuperado el 18 de Febrero de 2020

Parraguez Kobek, L. (2017). *The State of Cybersecurity in Mexico: An Overview.* Mexico: Wilson Center's Mexico Institute. Recuperado el 1 de Febrero de 2020, de https://www.wilsoncenter.org/sites/default/files/cybersecurity_in_mexico_an_overview.pdf

Pérez, F. (2019). *Riesgo Cibernético y Ciberseguridad.* Secretaría de Hacienda y Crédito Público. CNSF. Recuperado el 22 de Mayo de 2020, de https://www.gob.mx/cms/uploads/attachment/file/478193/181.-_Riesgo_Cibern_tico_y_Ciberseguridad_2019.pdf

PROSIC. (2010). *Ciberseguridad en Costa Rica.* San José: Universidad de Costa Rica. Recuperado el 4 de Febrero de 2020, de http://www.prosic.ucr.ac.cr/sites/default/files/documentos/ciberseguridad_2010.pdf

Quecedo, R., & Castaño, C. (2002). Introducción a la metodología de investigación cualitativa. *Revista de Psicodidáctica*, págs. 5-39. Recuperado el 18 de Febrero de 2020, de https://www.redalyc.org/pdf/175/17501402.pdf

Quirós-Ramírez, A. (2019). *Informe Hacia la Sociedad de la Información y el Conocimiento 2018.* Universidad de Costa Rica. Programa Sociedad de la Información y el Conocimiento. Recuperado el 17 de Mayo de 2020, de http://www.prosic.ucr.ac.cr/informe-hacia-la-sociedad-de-la-informacion-y-el-conocimiento-2018

Reis Balboni, M., Guerra, M., Cristancho, C., & Sánchez, M. (Octubre de 2009). *Indicadores para la Sociedad de la Información en América Latina y el Caribe: Avances y desafíos en la medición del acceso y uso de las TIC.* Salvador de Bahía, Brasil: CEPAL. Recuperado el 1 de Febrero de 2020, de CEPAL: https://www.cepal.org/socinfo/noticias/noticias/7/37627/Indicadores_para_SocInfo_en_ALC_Avancesydesaf%C3%ADos_CLAD2009.pdf

Romero Galicia, J. (2018). *Conceptualización de una estrategia de ciberseguridad para la Seguridad Nacional de México.* México: Universidad Autónoma de Tamaulipas. Recuperado el 10 de Febrero de 2020, de https://www.redalyc.org/jatsRepo/654/65458498003/html/index.html

Serrano, A., & Martínez, E. (2003). *La Brecha Digital: Mitos y Realidades.* Baja California, Mexico: Editorial Universitaria de la Universidad Autonoma de Baja California. Recuperado el 12 de Mayo de 2020, de http://www.labrechadigital.org/labrecha/LaBrechaDigital_MitosyRealidades.pdf

Sierra, F. (2003). La guerra en la era de la información: propaganda, violencia simbólica y desarrollo panóptico del sistema global de comunicación. *Sphera Pública*, págs. 253-268. Recuperado el 15 de Mayo de 2020, de https://www.redalyc.org/pdf/297/29700314.pdf

The Council of Economic Advisers. (2018). *The Cost of Malicious Cyber Activity to the U.S. Economy.* Executive Office of the President of the United States . Recuperado el 1 de Febrero de 2020, de https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

The White House. (2018). *National Cyber Strategy of th United States of America.* Washington: The White House. Recuperado el 2 de Febrero de 2020, de https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

Tovar, H. (2010). *Guerra de la información ¿El arma es el mensaje?* Universidad Central de Venezuela. Recuperado el 15 de Mayo de 2020, de https://www.academia.edu/9271831/Guerra_de_Informaci%C3%B3n_el_arma_es_el_mensaje

United States Executive Office of the President. (2009). *Cyberspace policy review: Assuring a trusted and resilient information and communications infrastructure.* United States Executive Office of the President. Recuperado el 20 de Mayo de 2020, de https://fas.org/irp/eprint/cyber-review.pdf

Valverde, R. (5 de Junio de 2019). *Costa Rica sufrió 19 millones de ataques cibernéticos los primeros tres meses del 2019.* Recuperado el 2 de Febrero de 2020, de Semanario Universidad: https://semanariouniversidad.com/tecnologia/costa-rica-sufrio-19-millones-de-ataques-ciberneticos-los-primeros-tres-meses-del-2019/

Vásquez, A. (2008). Zygmunt Bauman: Modernidad Liquida y fragilidad humana. *Revista Crítica de Ciencias Sociales y Jurídicas*(3). Recuperado el 11 de Mayo de 2020, de https://revistas.ucm.es/index.php/NOMA/article/download/NOMA0808320309A/26351