FACULTAD DE DERECHO

PROYECTO LEGAL PARA UN ESQUEMA NACIONAL DE CIBER SEGURIDAD

PRESENTADO POR

RAFAEL GUSTAVO PARRA PEREA

ASESOR: GINNO CASTELLANOS FERNÁNDEZ

TESIS

PARA OPTAR EL TÍTULO PROFESIONAL DE ABOGADO

LIMA – PERÚ

2016

UNIVERSIDAD DE SAN MARTÍN DE PORRES

FACULTAD DE DERECHO

"PROYECTO LEGAL PARA UN ESQUEMA NACIONAL DE CIBER SEGURIDAD"

Tesis para optar el Título Profesional de Abogado

AUTOR

RAFAEL PARRA

ASESOR

DR. GINNO CASTELLANOS FERNANDEZ

LIMA – PERÚ

2016

Sé extremadamente sutil, discreto, hasta el punto de no tener forma.
Sé completamente misterioso y confidencial, hasta el punto de ser silencioso.
De esta manera podrás dirigir el destino de tus adversarios.
(Sun Tzu, El arte de la Guerra, 550 – 500 a.c)

INDICE

Primer Capítulo

Segundo Capitulo

Tercer Capítulo

Cuarto Capitulo

Quinto Capitulo

Parte Final

INTRODUCCIÓN

Área de Investigación.-

La investigación se relaciona con las áreas de Derecho Cibernético, Derecho Informático, Defensa Nacional.

Tema de Investigación.-

Realizar un análisis sobre el desarrollo cibernético e informático que el Estado Peruano debe de atender como principal garante de la Seguridad Nacional, adoptando las medidas necesarias para implementar y aplicar una legislación acorde a la realidad internacional.

Desarrollar un análisis de los Ciber Delitos que organizaciones internacional como *ICANN*[1], *Anti-Phishing Working Group APWG*[2]*, Trend Micro*[3] *o el CICTE*[4] *de la OEA* consideran como delitos, así como el impacto negativo que ataques anteriores han tenido en la economía de un Estado.

Nos condujo a la elección de un tema que llamo nuestra especial atención dentro de las modernas tendencias del Derecho cibernético: *Proyecto legal en un esquema Nacional de Ciber seguridad.*

Título de Investigación.-

"PROYECTO LEGAL PARA UN ESQUEMA NACIONAL DE CIBER SEGURIDAD"

---

[1] ICANN, responsable de la coordinación global del sistema de identificadores únicos de Internet y de su funcionamiento estable y seguro, *Internet Corporation for Assigned Names and Numbers* - La Corporación de Internet para la Asignación de Nombres y Números.

[2] APWG, agrupación internacional que reúne a las empresas afectadas por los ataques de phishing, productos de seguridad y empresas de servicios, agencias gubernamentales, asociaciones comerciales, las organizaciones regionales de tratados internacionales y de las empresas de comunicaciones.

[3] TREND MICRO, Empresa dedicada al desarrollo de software de Ciber seguridad a nivel mundial, actualmente consultora de Ciber Seguridad de la OEA.

[4] CICTE OEA, Comité Interamericano contra el Terrorismo de la Organización de Estados Americanos.

Planteamiento del Problema de Investigación.-

Descripción del Problema de investigación

La dinámica internacional y el avance de las Tecnologías de la Información y de las Comunicaciones (*TIC*) ponen en manifiesta desprotección a personas (consumidores de servicios) como a empresa (prestadoras de servicios) y al Estado, haciendo necesario que el Sector Publico así como el Sector Privado cuenten con mecanismos legislativos, informáticos y cibernéticos que puedan afrontar de mejor manera los posibles Ciber Ataques.

Las *TIC*[5] y el Ciber espacio han desarrollado la forma de comunicarse de las personas, rompiendo la estática que existía en las comunicaciones y en el intercambio de información, haciendo posible que el mundo entero se encuentre en un punto en común, *El Ciber espacio.*

El Derecho debe de evolucionar con la realidad del momento en el que se aplica, es por ello que la Ciber Seguridad y la Ciber Defensa, deben ser conceptos que se encuentren ligados íntimamente con el concepto de Soberanía de Estado que es entendido por Antonio Remiro Brotons como*:*

> *"El conjunto de competencias atribuidas al Estado por el Derecho Internacional, ejercitables en un plano de independencia e igualdad respecto de los otros Estados"*[6] *,"…su manifestación más importante en las relaciones internacionales es la capacidad de los Estados para obligarse con otros y empeñar su responsabilidad internacional en caso de incumplimiento"*[7]*.*

Modificando o añadiendo un ámbito adicional en el cual el Estado puede ejercer su Soberanía. La realidad mundial nos muestra que los Ciber Ataques se encuentran en aumento, este hecho se encuentra relacionado con el

[5] TIC, Tecnologías de la Información y las Comunicaciones.
[6] REMIRO BROTONS, Antonio, Derecho Internacional (I), 1997, pp. 75
[7] REMIRO BROTONS, Antonio, Derecho Internacional (I), 1997, pp. 75

desarrollo de la Internet y de las *TIC*, haciendo que actividades delictivas en la internet sea cada vez más sencillo y atractivo realizarlas, esto debido al alto tránsito de usuarios que se encuentra en la *WEB*[8], aunado a la posibilidad de realizar ataques que generen una alta rentabilidad y con la seguridad de no poder ser detectado. Los Ciber Ataques no son un fenómeno nuevo, la *OTAN*[9] fue uno de los primeros Organismo de defensa internacional en anunciar mecanismos de Ciber Defensa en el 2007[10], surgiendo de esta forma la posibilidad de Cooperación entre Estado con el objetivo de preservar la Ciber Seguridad y la Ciber Defensa.

La investigación pretende demostrar que la Internet y las *TIC* han cambiado la realidad y la falta de regulación en materia Cibernética es un problema que se acrecentará en el futuro cercano, con un aumento exponencial de los Ciber crímenes y situaciones en donde la soberanía se vea afectada por situación de tensión entre la países, es por ello que a través del presente documento nos sumamos a las intenciones de la *OEA*[11], de la *OTAN*, de *TREND MICRO*, en otros, con respecto a que los países creen mecanismo de prevención, control, represión, y contra ataque, en situaciones donde a través de trabajos previamente establecidos se pueda aplicar una normativa viva que haga posible contra restar el daño en situaciones de tensión cibernética o ataque.

Preguntas de Investigación

Nuestra investigación pretende responder básicamente las siguientes interrogantes

1. ¿Cuál es la Diferencia entre Ciber Seguridad y Ciber Defensa?

2. ¿Por qué la Ciber Seguridad y la Ciber Defensa son de vital importancia para la Defensa del Estado?

3. ¿Qué busca proteger la Cibersoberanía?

[8] WEB, World Wide Web, Red Informática Mundial.
[9] OTAN, Organización del Tratado del Atlántico Norte, alianza militar intergubernamental.
[10] http://www.natolibguides.info/cybersecurity - Información obtenida el 03/10/2015
[11] Organización de Estados Americanos.

4. ¿Qué implica que un Estado no cuente con políticas de Ciberseguridad y Ciberdefensa?

Justificación de la Investigación

Es indudable que en una realidad como la del Perú es necesario implementar una mejor legislación con objetivos y metas orientadas a la prevención y a la detección de Ciber Delitos así como la identidad de sus actores, creando grupos de trabajo especializados en la materia que sean capaces de administrar y preservar la Ciber Defensa y la Ciber Seguridad dentro del espacio Soberano del Perú. Esta nueva tendencia cibernética crea un ambiente en el que jurídicamente es necesario implementar los mecanismos de control, buscando reducir el impacto negativo dentro de la sociedad, reduciendo las pérdidas económicas en una posible situación de ataque.

El Perú actualmente cuenta con un organismo especializado *PeCERT*[12]**,** el cual tiene como función elevar los niveles de seguridad de la información en el sector público, no contando con un respaldo normativo acorde para ampliar sus objetivos para aportar y desarrollar mejor sus funciones.

El segundo organismo abanderado en materia cibernética es la *ONGEI*, es el ente rector del Sistema Nacional de Información, desarrollando su actividad en materia de Gobierno Electrónico o *eGobernence*[13], así como brindar asesoría a entidades estatales en materia informática. Con respecto a su función permanente se encuentra la normatividad informática.

A pesar de tener avances en materia cibernética, el Perú a nivel internacional no es considerado como un país que genere las condiciones necesarias para

[12] PeCERT, Sistema de Coordinación de la Administración Publica, encargado de liderar los esfuerzos para resolver, anticipar y enfrentar los ciber desafíos y coordinar la defensa ante los Ciber ataques, con el fin de proveer a la Nación de una postura segura en el ámbito de la seguridad informática.

[13] eGovernence, es la aplicación de tecnologías de la información y la comunicación (TIC) para la entrega de servicios gubernamentales, el intercambio de transacciones de comunicación de la información, la integración de los diversos sistemas y servicios independientes entre gobierno-a- cliente

mejor el campo de la Ciber Seguridad, pudiendo en esta materia crear un CIBER COMANDO o COMANDO CIBERNETICO, encargado de velar por la seguridad tanto a nivel interno como en situaciones de guerra o tensión con países vecinos, en el Perú el organismo más cercano a un Comando Cibernético es el *PeCERT*.

El Perú recientemente aprobó leyes que mejorarían nuestra realidad en materia de Ciber Crímenes, como son:

- La ley que incorporó los delitos cibernéticos al código penal – Ley 27309 derogada por la ley la 30096 Ley de Delitos Cibernéticos
- La ley de protección de datos personales – Ley 29733.

Según el reporte de *REPORTE DE SEGURIDAD CIBERNÉTICA E INFRAESTRUCTURA CRÍTICA DE LAS AMÉRICAS*[14], el Perú ha sufrido ataque cibernéticos (ICS/SCADA) y según el mismo reporte el Perú cuenta con una calificación de "ALGO PREPARADO" para afrontar Ciber ataques y según la OEA el Perú no ha aumentado el presupuesto para este sector en el periodo 2014 – 2015.

Según la *OEA* en *TENDENCIAS DE SEGURIDAD CIBERNETICA EN AMERICA LATINA Y EL CARIBE*, "el Perú no cuenta con una estrategia o política nacional oficial de seguridad cibernética"[15], es por ello que nuestra investigación pretende profundizar en materia de Defensa y Seguridad mostrando que el Perú actualmente necesita implementar mecanismo necesarios para afrontar incidentes que puedan ocurrir en un futuro cercano a través de la internet o de las *TIC*.

Hipótesis

[14] OEA – TREND MICRO, Reporte sobre Seguridad Cibernética e Infraestructura Crítica en las Américas, Abril 2015.
[15] OEA – Tendencia de seguridad cibernética en américa latina y el caribe, pp. 76.

La realización de la presente tesis llevara consigo, demostrar como el desarrollo tecnológico que viene aumentando a través de la Internet afecta o podría exponernos en una situación de peligro o de vulnerabilidad ante situaciones o incidente ocurridos en que tengan como medio a la internet o a las TIC´s, y como esta podría repercutir en la soberanía de los Estado, cuando se utiliza con fines ilícitos para la comisión de delitos.
Así mismo nuestra investigación llevará consigo el demostrar la necesidad de implementar mecanismos jurídicos y técnicos para abordar de mejor manera situaciones de ataque en *Infraestructuras Criticas*[16].

Motivación

La motivación que nos lleva a realizar la presente investigación es la falta de regulación específica en materia de Ciber Seguridad y Ciber Defensa, específicamente en las situaciones de ataque, en donde el Estado se encuentre en una situación de vulnerabilidad por la falta de mecanismos, que se encuentren acorde con la realidad actual.

Marco Teórico

Se utilizara como base los pronunciamientos de Organismos Nacionales como la *ONGEI*[17], así como de Organismos Internacionales como el *CICTE* y la *OTAN*. Así mismo se tomara como base las referencias de una empresa como *TREND MICRO*, encargada de la Ciber Seguridad y Ciber Defensa a nivel Internacional. Tomaremos en cuenta los reportes del *CAEM – Colombia*[18], como referente de técnicas avanzadas en Ciber Defensa y utilizaremos como referencia las publicaciones de revistas como *CYBER DEFENSE,* así como los avances en materia de Ciber Defensa de España y Colombia.

[16] Infraestructuras Criticas, conjunto de recursos, servicios, tecnologías de la información y redes, que en el caso de sufrir un ataque, causarían gran impacto en la seguridad, tanto física como económica, de los ciudadanos o en el buen funcionamiento del Gobierno de la Nación.
[17] ONGEI, es el Órgano Técnico Especializado que depende directamente del Despacho de la Presidencia del Consejo de Ministros (PCM) se encarga de liderar los proyectos, la normatividad, y las diversas actividades que en materia de Gobierno Electrónico realiza el Estado.
[18] CAEM, Curso de Altos Estudios Militares – Colombia.

Estado de la Cuestión

No existe en nuestro país regulación actualizada al respecto. Sin embargo se ha encontrado información en países de la región, por lo que este trabajo buscará mostrar algunos procedimientos en países de habla hispánica, inglesa y francófona, donde existen herramientas que podrían ser incorporados a nuestra legislación.

Metodología

La metodología a trabajar es la metodología exploratoria, ya que no existen estudios al respecto de Perú y lo que busca esta tesis es vislumbrar el camino para que otros investigadores, generen en el futuro una mejora en la regulación actual.

PRIMER CAPITULO

1. Antecedentes Históricos a nivel Internacional

Los Ciber ataques son hechos que responden a la revolución tecnológica, son sucesos que viene cambiando la realidad en la que nos encontramos. En esta realidad no debe sorprendernos que las modalidades de cometer ilícitos o atacar determinadas infraestructuras críticas sea atractivo para las personas y organizaciones a nivel mundial que buscar generarse un provecho mediante este tipo de acciones.

Al inicio de toda esta revolución tecnológica los *HACKERS*[19] no realizaban sus actividades buscando el provecho económico o el daño masivo que se conoce ahora, con lo que la presente sección pretende acercarnos al inicio de la *CIBERCRIMINALIDAD.*

El punto de partida de la presente investigación será el *CIBERATAQUES* conocido como *Morris WORM*[20], la *OTAN*[21] registró este hecho como el primer *CIBERATAQUE perpetrado por un civil, el cual buscaba "saber que tan grande era la internet"*, ocurrido en 1988, fue realizado por Robert Tapan Morris, creador de *Morris WORM*[22], este fue el primer *MALWARE*[23] conocidos que buscaba atacar la infraestructura naciente de la Internet, expandiéndose a través de ordenadores de todo el mundo, el efecto principal que causaba este *MALWARE*[24] era el desacelerar los ordenadores hasta el punto de dejarlos inservibles. En noviembre de 1988, aproximadamente 6000 ordenadores

---

[19] m. y f. Inform. pirata informático - RAE

[20] NATO.INT - Portal de la OTAN - http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm - sitio visitado 25/02/2016.

[21] Organización del Tratado del Atlántico Norte

[22] Morris Worm: es el nombre que se asignó al software creado por Robert Tapan Morris

[23] Malware: software malicioso, código maligno, cuyo objetivo es infiltrase en o dañar una computadora sin el consentimiento de su propietario.

[24] Malware.- llamado *badware*, código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario.

fueron infectados entre los afectados se encontraba el Centro de Investigación de la *NASA*[25].

Es difícil imagina después de los acontecimiento que ocurren actualmente que una persona con alguna habilidad técnica en sistemas de *HARDWARE*[26] *o SOFTWARE*[27] quiera atacar una infraestructura con el único objetivo de conocer sus dimensiones, de lo que en ese momento estaba teniendo sus primeros pasos, la *Internet.*

La línea de tiempo que utilizaremos para mostrar el desarrollo de los Ciber Ataques, muestra que una de las infraestructuras favoritas para atacar es la *NASA*. Esta entidad ha sido víctima de varios ataques a lo largo de la historia del internet, en el 2006 la Nasa fue víctima de un *CIBERATAQUE* forzando a bloquear sus sistemas de correo electrónico con archivos adjuntos, el ataque hizo que información sobre el lanzamiento al espacio de vehículos se filtrara.

Es necesario que nos detengamos a pensar sobre los daños que hubiera podido causar o podrían causar posibles *CIBERATAQUES* a un país como el Perú, el cual según reportes actuales de organismos internacionales, no cuenta con medidas preventivas de mitigación de riesgo antes posibles *CIBERATAQUES*, con lo cual es necesario analizar si las políticas de *CIBERDEFENSA* y *CIBERSEGURIDAD* que se plantean para la región podrían beneficiarnos si acogemos las recomendaciones realizadas por estos Organismos especializados, con lo dicho no pretendemos alarma ante la situación de indefensión en la cual nos encontramos, pero si buscamos que se tomen las medidas necesarias para comenzar el cambio ante las crecientes amenazas que mostraremos más adelante.

[25] La Administración Nacional de la Aeronáutica y del Espacio - NASA.
[26] Hardware.- se refiere a todas las partes físicas de un sistema informático; sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos.
[27] Software.- E*quipo lógico o soporte lógico* de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas.

Continuando con la línea de tiempo, el siguiente *CIBERATAQUE* ocurrido fue en Estonia[28](2007) el cual fue realizado a través de *BOTNETS*[29] procedentes de todo el mundo, los cuales enviaban solicitudes a un servidor obteniendo como resultado que el servidor atacado se encuentre incapaz de aceptar nuevas conexiones y quede inhabilitado. El ataque tuvo como objetivos: Las páginas web del Presidente de Estonia, del Parlamento de Ministros Gubernamentales y de las Organizaciones de noticias, a pesar que el ataque al parecer tuvo como objetivo entidades gubernamentales, algunos bancos reportaron que sufrieron ataques, generando así perdidas monetarias que ascienden al millón de dólares[30]. El ataque se desarrolló en medio de una realidad internacional convulsionada, con tensión entre Estonia y Rusia, por lo cual se le acredita la autoría del ataque.

Estonia es un hito histórico el cual no puede pasar desapercibido para la experiencia internacional, en donde en una situación de tensión entre países y sin previamente haber emitido alguna declaración de guerra, uno de ellos ataca a otro, inhabilitando parte del país, y generando pérdidas en el sistema financiero, con lo cual una vez más, la investigación pretende generar conciencia de lo ocurrido en el pasado para poder llegar a un futuro con unos sistema que permitan reducir el impacto ante una situación la cual es cada vez más real.

La peligrosidad de los ataques realizados a través del *CIBERESPACIO*, como vemos en la presente investigación, tiene límites, pero los límites que se conocen están relacionados en la medida en que tan conectados estemos al *CIBERESPACIO*, es decir, mientras más dependientes seamos de los sistemas cibernéticos más vulnerables nos encontraremos antes la *CIBERDELINCUENCIA*, como ejemplo podemos tomar el ciberataque que tuvo como objeto al **Secretario de Defensa de los Estados Unidos de**

---

[28] NATO.INT – Portal de la OTAN, http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm, Información sustraída: 25/02/2016.

[29] Botnet: término utilizado para hacer referencia a un conjunto de Robots, que se ejecutan de manera autónoma y automática. El operador de la botnet puede controlar remotamente todos los ordenadores o servidores.

[30] Información Obtenida de:https://www.technologyreview.es/blog/359/31216/los-20-ciberataques-mas-perversos-del-siglo-xxi/ Visitado el 19/12/2015.

Norte América (2007), al cual le hackearon[31] la cuenta de correo electrónico para acceder a información clasificada del Pentágono. [32]

Se hace necesario plantear la pregunta: *¿LOS OBJETIVOS DE LOS CIBERATAQUES SON CIVILES, PERSONAL DEL ESTADO, O INFRAESTRUCTURAS CRITICAS?* la respuesta la obtendremos en base a lo que busca el *CIBERDELINCUENTE*, actualmente no podemos hablar de un patrón para predecir algún *CIBERATAQUE*, es posible que la estrategia de ataques sea la población civil para a través de sus ordenadores hacer colapsar servidores de diferentes entidades publica (Infraestructuras Criticas[33]), este *CIBERATAQUE* es conocido como *Botnets.*[34]

Las *Infraestructuras Criticas* a nivel mundial representan la parte más sensible en la organización estatal, es muchas veces a través de ellas que se puede generar los mayores CIBERATAQUES con los más altos índices de daño al Estado, tal es el caso de China que en octubre del 2007 sufrió un *Ciberataque*, en el cual se robó información de áreas claves de ***China Aerospace Science & Industry Corporation*** *(CASIC)*[35], el ataque fue realizado a través de Spyware[36] instalados en computadores de departamento que almacenaban información clasificada y de algunos altos cargos, el objetivo fue sustraer información, se le acredito la autoría a Hackers extranjeros.

Las Infraestructuras Criticas, no siempre son entidades públicas como Ministerios o Superintendencias, también pueden ser empresas privadas como fondos de pensiones o bancos, pero esto no impide que el

[31] Hackear.- significa acción de irrumpir o entrar de manera forzada a un sistema de cómputo o a una red.
[32] Pentagono.- El Pentágono es la sede del Departamento de Defensa de los Estados Unidos.
[33] Infraestructuras Críticas.- sistemas físicos o virtuales y activos bajo la jurisdicción de un Estado que son tan vitales que su incapacitación o destrucción pueden debilitar la seguridad, la economía, la salud de un Estado o la seguridad pública o el medio ambiente.
[34] Botnets.- es un término que hace referencia a un conjunto o red de *robots informáticos* o *bots*, que se ejecutan de manera autónoma y automática.[1] El artífice de la botnet puede controlar todos los ordenadores/servidores infectados de forma remota.
[35] China Aerospace Science & Industry Corporation (CASIC).- Ciencia Aeroespcial de China e Corporacion Industrial.
[36] Spyware.- es un malware que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador.

CIBERCRIMINAL excluya a objetivos distintos como lo ocurrido en la **Campaña Electoral de Estados Unidos** (2008), según el informe de la OTAN no se le ha atribuido este hecho a algún Hacker, el objetivo fue una base de datos de las dos listas presidenciales, Democrática y Republicana.[37]

Así como estos hechos la *OTAN* registró hechos ocurridos alrededor del mundo, las cuales ordenaremos en la siguiente relación:

- ✓ Las redes de ordenadores en Georgia[38] fueron hackeados por intrusos extranjeros (2008), estos hechos ocurrieron durante un conflicto con Rusia, el ataque no tuvo gran impacto, lo que apareció fue un *Grafiti*[39]en la página del Gobierno de Georgia.

- ✓ Hackers atacan la infraestructura de internet de Israel[40] (2009), los hackers atacan la infraestructura de Internet israelí durante la ofensiva militar de enero de 2009 en la Franja de Gaza. El ataque, que se centró en los sitios web del gobierno, fue ejecutado por al menos 5.000.000 de computadoras. Los funcionarios israelíes creían que el ataque fue llevado a cabo por una organización criminal con base en un antiguo estado soviético, y pagado por Hamas[41] o Hezbolá[42].

---

[37] NATO.INT – Portal de la OTAN, http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm, Información sustraída: 25/02/2016.

[38] NATO.INT – Portal de la OTAN, http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm, Información sustraída: 25/02/2016.

[39] Grafiti.- Una modalidad de pintura libre, destacada por su ilegalidad, generalmente realizadas en espacios urbanos.

[40] NATO.INT – Portal de la OTAN, http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm, Información sustraída: 25/02/2016.

[41] Hamas.- es una organización palestina que se declara como yihadista, nacionalista e islámica. Su objetivo, definido en su carta fundacional, es el establecimiento de un estado islámico en la región histórica de Palestina, que comprendería los actuales Israel, Cisjordania y la Franja de Gaza, con capital en Jerusalén.

[42] Hezbola.- es una organización musulmana libanesa que cuenta con un brazo político y otro paramilitar. Fue fundado en el Líbano en 1982 como respuesta a la intervención israelí de ese momento y fueron entrenados, organizados y fundados por un contingente de la Guardia Revolucionaria iraní.

- ✓ Grupo llamado "Ciber Ejército Iraní" atacó Baidu[43], (2010) interrumpió el servicio del *Buscador* chino **Baidu** populares. Los usuarios se redirigen a una página que muestra un mensaje político iraní. El mismo "Cyber Ejército iraní" había cortado en Twitter el mes de diciembre anterior, con un mensaje similar.

- ✓ Stuxnet[44] (2010), Stuxnet, una pieza compleja de *Malware* diseñado para interferir con los sistemas de control industrial Siemens, fue descubierto en Irán, Indonesia, y en otros lugares, lo que lleva a la especulación de que se trataba de un arma cibernética del gobierno dirigida a el programa nuclear iraní.

- ✓ Canadá reporto el mayor Ciber ataque contra sus agencias[45] (2011), incluyendo la Defensa de Investigación y Desarrollo de Canadá, una agencia de investigación para el Departamento de Defensa Nacional de Canadá. El ataque obligó al Departamento de Finanzas y del Consejo del Tesoro, los principales organismos económicos de Canadá, para desconectarse de Internet.

- ✓ Departamento de Defensa de los Estados Unidos de Norte América[46] fue atacado (2011), en un discurso revelando la estrategia cibernética del Departamento de Defensa, el subsecretario de Defensa mencionó que un contratista de defensa fue hackeado y 24.000 archivos del Departamento de Defensa fueron robados.

---

[43] NATO.INT – Portal de la OTAN, http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm, Información sustraída: 25/02/2016.
[44] Loc. Cit. http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm, Información sustraída: 25/02/2016.
[45] Loc. Cit. http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm, Información sustraída: 25/02/2016.
[46] NATO.INT – Portal de la OTAN, http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm, Información sustraída: 25/02/2016.

- ✓ Octubre Rojo[47] (2012), La empresa rusa Kaspersky descubrió un ataque cibernético en todo el mundo llamado "Octubre Rojo", que había estado funcionando por lo menos desde 2007. Los hackers reunieron información a través de vulnerabilidades en los programas Microsoft Word y Excel. Los objetivos principales de los ataques parecen ser los países de Europa del Este, la ex Unión Soviética y Asia Central, aunque Europa occidental y América del Norte reportaron víctimas también. El virus recogió información de embajadas gubernamentales, empresas de investigación, instalaciones militares, proveedores de energía, nucleares y otras infraestructuras críticas.

- ✓ Ataque a Corea del Sur[48] (2013), instituciones financieras de Corea del Sur, así como el organismo de radiodifusión de Corea YTN tenían sus redes infectadas en un incidente considerado semejante a los esfuerzos pasados cibernéticos por parte de Corea del Norte.

2. Conceptualización histórica

Si bien los *CIBERATAQUES*, son la actividad negativa y son una creación humana, *INTERNET*. Es necesario tener en cuenta que la *INTERNET*, es una herramienta, que ha colaborado con el desarrollo de la humanidad, haciendo posible romper los límites físicos conocidos, acercando personas, empresas y países.

La tecnología que en un origen creo la *INTERNET* ahora ha desarrollado otro tipo de actividades. Estas actividades dependen del *USUARIO*, y de los conocimientos que tenga para desarrollarlas, sean estas con fines lícitos como ilícitos.

[47] Loc. Cit. http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm, Información sustraída: 25/02/2016.
[48] Loc. Cit. http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm, Información sustraída: 25/02/2016.

A nivel mundial se han creado diferentes organizaciones que buscan hacerle frente a los *CIBERDELINCUENTES*, como el FBI, que es una organización gubernamental que busca proteger, reconoce y educar a la población, para así tener una mejor posición frente a personas con habilidades especiales que las utilizan de manera negativa, es necesario capacitar a los *USUARIOS* brindando herramientas sencillas que servirán para reportar algún *INCIDENTE*, así el FBI podrá reconocer a los *CIBERATAQUES,* el FBI de la siguiente forma:

> *"A cyber incident is a past, ongoing, or threatened intrusion, disruption, or other event that impairs or is likely to impair the confidentiality, integrity, or availability of electronic information, information systems, services, or networks. SLTT partners are encouraged to voluntarily report suspected or confirmed cyber incidents to a federal entity. In particular, a cyber incident should be reported if it:*
>
> - *May impact national security, economic security, or public health and safety.*
> - *Affects core government or critical infrastructure functions.*
> - *Results in a significant loss of data, system availability, or control of systems.*
> - *Involves a large number of victims.*
> - *Indicates unauthorized access to, or malicious software present on, critical information technology systems.*
> - *Violates federal or SLTT law."*[49]
> -
>
> *"Un incidente cibernético es un hecho pasado, o la intrusión en curso, amenaza o alteración, o cualquier otro evento que afecte o pueda mermar la confidencialidad, integridad o disponibilidad de la información electrónica, sistemas de*

[49] FBI.GOV – Portal del FBI, https://www.fbi.gov/about-us/investigate/cyber/law-enforcement-cyber-incident-reporting, Información sustraída: 16/04/2016

información, servicios y redes. SLTT[50] Se anima a los socios a informar sobre sospechas de forma voluntaria o la confirmación de CIBERINCIDENTES a una entidad federal. En particular, un CIBERINCIDENTE se debe informar si:

- *Puede afectar la seguridad nacional, la seguridad económica, o público salud y seguridad.*
- *Afecta al gobierno central o funciones de infraestructura crítica.*
- *Resulta en una pérdida significativa de datos, la disponibilidad del sistema, o control de los sistemas.*
- *Consiste en un gran número de víctimas.*
- *Indica el acceso no autorizado, o software malicioso presentar en adelante, los sistemas críticos de tecnología de la información.*
- *Viola la ley federal o SLTT."*[51]

EL FBI nos muestra lo que es una intrusión *CIBERNETICA*, lo cual capta nuestra atención, debido a que no utiliza el término *INFORMATICO*, esto hace que nos preguntemos: ¿POR QUE EL FBI UTILIZA EL TERMINO CIBERNETICO EN VES DEL TERMINO INFORMATICO? La respuesta la desarrollaremos a profundidad más adelante, pero como adelanto comentaremos lo siguiente, ***que los incidentes CIBERNETCOS son hechos que los CIBERDELINCUENTES realizan para generarse oportunidades a través de posibles vulnerabilidades en sistemas informáticos.*** El FBI establece parámetros de *CIBERSEGURIDAD* que son como directrices que marcan como actuar frente a determinadas situaciones.

Actualmente uno de los países de la región que marca la pauta, con respecto a los avances de la ciberseguridad y ciberdefensa es Colombia, por ello consideramos necesario establecer el concepto de *CIBERSEGURIDAD*, según la experiencia Colombiana, a través del Documento publicado por el Ministerio de Tecnologías de la Información y las Comunicaciones, no dice:

[50] SLTT .- Siglas en inglés: State, Local, Tribal and Territorial Goverment - Estatales, locales, tribales y territoriales Gobierno
[51] Google traductor – Del Inglés al Español.

> *"…se define la ciberseguridad como la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética."*[52]

La *CIBERSEGURIDAD* tendría que ser una actividad Estatal de necesaria atención a nivel mundial, una vez más la experiencia Colombiana nos dice:

> *"La continua evolución, crecimiento y sofisticación de los ataques cibernéticos, al igual que la convergencia tecnológica, ponen de manifiesto la necesidad de adoptar las medidas y controles que permitan proteger al Estado y a la ciudadanía en general ante estas nuevas amenazas. El aumento de la capacidad delincuencial en el ciberespacio, así como la utilización de nuevas tecnologías para generar amenazas informáticas, constituyen una preocupación común a todos los países y Colombia no es la excepción, dado que impactan de manera significativa la seguridad de la información, en los ámbitos tanto público como privado e incluyendo a la sociedad civil."*[53]

3. Primer Ciber ataque conocido

A lo largo de la historia de la humanidad se han reportado conflictos he incidentes violentos, como por ejemplo *La Primer Acción de Guerra de la Historia de la Humanidad*[54], el hecho ocurrió en Kenia ya hace 10,000 años, pero como todo va en evolución la diferencia entre esta *Primer Acción de Guerra* y los ataques que se realizan en la actualidad es que en los actuales muchas veces no podemos saber de dónde viene el ataque y quien o quienes lo realizan, esto y que las herramientas que se utilizan actualmente no tiene

---

[52] Ministerio de Tecnología de la Información y las Comunicaciones, Agenda estratégica de Innovación: Ciberseguridad (2014) pp. 4.
[53] Loc. Cit. Idem.
[54] Información sustraída de: http://www.lavanguardia.com/ciencia/20160120/301550503459/descubierta-en-kenia-la-primera-accion-de-guerra-de-la-historia-de-la-humanidad.html. Información sustraída: 27/02/2016

filo y no rompen huesos si no seguridades cibernéticas en sistemas, tomando diversas vulnerabilidades para poder llegar a obtener lo que se busca.

Así podemos tomar como referencia para establecer el primer *ciberataque* conocido lo reportado por dos entidades: *The Federal Bureau of Investigation – FBI,* y la *Organización del Tratado del Atlántico Norte* – OTAN.

Se hace necesario comentar que alrededor del mundo se han suscitado diversos casos relacionados a c*iberataques,* siendo algunos puestos a conocimiento del público, y otro manteniéndose en privado, por considerarse que son temas *de SEGURIDAD NACIONAL*, motivo por el cual no han sido develados[55].

En definitiva, es bueno compartir las experiencias relacionadas a ciberataques con la población, siempre y cuando no se expongan las vulnerabilidades de las entidades o Estados afectados, el límite será siempre establecido al ponderar el derecho de informarnos con la seguridad nacional.

Es así que por parte del *FBI* tenemos la siguiente lista de *Ciber Ataques:*

- AUSTRALIA
  - ✓ Según Brian Boeting, miembro del FBI – San Francisco, en el año 2000, una persona obtuvo el control de una planta de tratamiento de desagüe cloacal y libero un millón de litros de desechos en los ríos, siendo este uno de los Ciberdelitos más sonados en el mundo[56].

  - ✓ El 15 de abril de 2010, la compañía de telecomunicaciones *OCPUS* sufrió un ataque por parte de China. Se dice que fue un ataque "por error"[57].

[55] Ing. Jhon Cesar Arango, Gerente de Proyectos de ITforensic LTDA, se le formuló una pregunta en referencia a los Delitos de Terrorismo Informático en su país. No contesto dicha pregunta, pues afirma que por medidas de seguridad y contratos laborales, no está autorizado para hablar sobre el tema.
[56] INI, Fedrico. Reportaje perteneciente al Programa Televisivo "Informe Central" conducido por Rolando Graña (24/01/2007) "Ciberterrorismo, ¿Mito o Realidad?. En: http://www.youtube.com/watch?v=h4a_QIwbRjE Información sustraída: 27/02/2016.
[57] elEconomista.es: Telecomunicaciones y Tecnología. "China lanza un Ciberataque contra una teleco australiana por error". Publicado el 15 de abril de 2010. En: http://

- ✓ El 13 de marzo de 2011 es atacado el Banco Central de Australia, se dice que fue por parte de China y que la finalidad era robar información sobre planes económicos de este y otros países. El *malware* que se utilizó para infectar los ordenadores es de origen chino y su función era recolectar información sobre las negociaciones del G20 en 2011. Los correos electrónicos desarrollados por los *Hackers*[58], que contenían un troyano, incluían una firma de correo legítima y su contenido y título eran posibles. El asunto de los mensajes era "Planificaciones Estratégicas FY2012" y el remitente era supuestamente un importante ejecutivo del banco[59].

- ESTADOS UNIDOS
  - ✓ Organismos de seguridad como el FBI o la CIA han informados de diversos *Ciber Ataques* que sufrió Estados Unidos; sin embargo, ninguno ha surtido efectos gracias al gran sistema de defensa que vienen desarrollando en los Medios Informáticos[60]. El número de ataques que ha recibido Estados Unidos es desconocido hasta la actualidad.

  - ✓ Así mismo se hizo el anuncio por parte de la Marina de los Estados Unidos de la formación de un nuevo escuadrón de *EJERCITO INFORMATICO*[61]*,* equipo preparado para la *CIBERDEFENSA* del Estado y la lucha en la *CIBERGUERRA.*

¿eciduario.eleconomista.es/telecomunicaciones-tecnologia/noticias/2061591/04/10/China-lanza-un-ciberataque-contra-una-teleco-australiana-por-error.html Información sustraída: 27/02/2016.

[58] Término utilizado "hacker" o "pirata informático" es utilizado para referirse a personas apasionadas en el ambiente de la Seguridad Informática, programadores y diseñadores, en su mayoría el termino es utilizado de manera errónea, siendo empleado para referirse en su mayoría a los criminales informáticos.

[59] JOYE, Christopher. The Australian Financial Review. "Cyber-Attacks penétrate Reserve Bank networks". Publicado el 11 de marzo de 2013. En: http://www.afr.com/p/national/cyber_attacks_penetrate_reserve"FEdCLOl50owRMgl0urEYnK

[60] Fedrico. Reportaje perteneciente al Programa Televisivo "Informe Central" conducido por Rolando Graña (24/01/2007) "Ciberterrorismo, ¿Mito o Realidad?. En: http://www.youtube.com/watch?v=h4a_QIwbRjE Información sustraída: 27/02/2016

[61] Fedrico. Reportaje perteneciente al Programa Televisivo "Informe Central" conducido por Rolando Graña (24/01/2007) "Ciberterrorismo, ¿Mito o Realidad?. En: http://www.youtube.com/watch?v=h4a_QIwbRjE Información sustraída: 27/02/2016

- COLOMBIA
  - ✓ En 2011, se realizó un ataque *CIBERTERRORISTA,* en protesta por una ley impulsada por el presidente de Colombia, Juan Manuel Santos, que buscaba penalizar el terrorismo en internet[62].

- ESPAÑA
  - ✓ Actores "Antifascistas" que se les podría denominar Terroristas Informáticos, publican datos de clientes comercios sevillanos para ser objetivos de sus acciones. La *COORDINADORA DE SEVILLA CON EL TERRORISMO (CSCT)* tuvo conocimiento que varios establecimiento comerciales de moda y souvenirs, habrían sido víctima de una ataque informático a sus webs y bases de datos de clientes con el fin de robar la información de sus clientes, muchos de ellos miembros de las fuerzas y cuerpos de seguridad del Estado, para colgarlos en webs y sitios de internet violentos y extremistas vinculados a grupos autodenominados "antifascistas", la acción buscaba que se actué en contra de esos clientes por comprar prendas o motivos con la bandera de España y otro símbolos de España[63].

La experiencia internacional en materia de ataques cibernéticos se está desarrollando, y gracias a la cooperación de organismos internacionales así como la experiencia compartida de los Estado hace posible que la *Ciber Defensa y la Ciber Seguridad* se desarrollen.

Por otro lado la OTAN, como ya lo mencionamos líneas arriba, hace una línea de tiempo bastante ilustrativa para entender desde sus inicios a los *Ciber Ataques*.

---

[62] LA GACETA, "Allanan la casa de un tucumano investigado por "Ciberterrorismo" contra el Ejército de Colombia" Publicado el 20 de Febrero de 2012. En: http://www.lagaceta.com.ar/nota/478615/allanan-casa-tucumano-investigado-ciberterrorismo-contra-ejercito-colombia.html Información sustraída: 27/02/2016

[63] OPERACIÓN CONTRA EL CIBERTERRORISMO. "terroristas Informáticos "Antifascistas" publican datos de clientes de comercios sevillanos para ser objetos de sus acciones". Publicado el 28 de Febrero de 2012. En: http://terroristasnogracias.blogspot.com/2012/02/operacion-contra-el-cibercrimen.html Información sustraída: 03/03/2016

Así tenemos los siguientes:

- EL GUSANO MORRIS – 1988
  - ✓ Uno de los primeros gusanos[64] reconocidos para afectar la infraestructura cibernética naciente del mundo - extendido alrededor de las computadoras en gran medida en los EE.UU.

  - ✓ El gusano utiliza las debilidades en el sistema UNIX Sustantivo 1[65] y se replica en sí con regularidad.

  - ✓ Se ralentizó ordenadores hasta el punto de ser inutilizable. El gusano fue obra de Robert Tappan Morris, quien dijo que sólo estaba tratando de medir qué tan grande era de Internet. Posteriormente se convirtió en la primera persona en ser condenada en virtud de fraude informático y el abuso de los EE.UU.

  - ✓ En la actualidad trabaja como profesor en el MIT.

- LA NASA – Diciembre 2006
  - ✓ Se vio obligado a bloquear mensajes de correo electrónico con archivos adjuntos antes de un lanzamiento fuera por el miedo a ser *Hackeado*.

  - ✓ Business Week[66] informó que los planes de los nuevos vehículos de lanzamiento espacial de Estados Unidos fueron obtenidos por intrusos extranjeros desconocidos.

- ESTONIA – Abril 2007
  - ✓ las redes del gobierno de Estonia fueron *Hackeadas* por un *ATAQUE DE DENEGACIÓN DE SERVICIO*[67] por parte de intrusos

[64] Gusano.- Un gusano informático es un malware que tiene la propiedad de duplicarse a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario.
[65] UNIX Sustantivo 1.- Es un sistema operativo portable, multitarea y multiusuario; desarrollado, en principio, en 1969, por un grupo de empleados de los laboratorios Bell de AT&T.
[66] Business Week.- Es una revista semanal de negocios publicada por Bloomberg L.P.

extranjeros desconocidos, por la eliminación de un monumento a los caídos Rusos.

- ✓ Algunos servicios en línea del gobierno fueron interrumpidos temporalmente como la banca en línea.

- ✓ Los ataques eran más como disturbios cibernéticos que los ataques paralizantes.

- ✓ El relanzamiento de algunos servicios en cuestión de horas o en la mayoría de los días.

4. Antecedentes Nacionales - Ciber Ataques – PERÚ

La presente sección de la investigación, es en teoría la parte más importante, hasta el momento, porque será gracias a esta sección que podremos comprender que como Estado no nos hemos mantenido al margen o ajenos en lo que a *Ciber Ataques* concierne, es más, el Perú con una historia tan convulsionada como la nuestra deberíamos estar mucho mejor preparados de lo que estamos actualmente.

Si bien el Perú es un Estado que como otros Estados está inmerso en la posibilidad de ser víctima de ataques cibernéticos, por la experiencia dejada por el *TERRORISMO,* debemos ser mucho más cuidadosos a la hora de emprender la laboriosa tarea de legislar los *DELITOS INFORMATICOS, crear DIRECTIVAS EN CIBER DEFENSA Y crear mecanismo de CIBER SEGURIDAD.*

En la actualidad, en el Perú se vienen cometiendo desde hace años el delito de *APOLOGIA AL TERRORISMO*, con el uso de Medios Electrónicos, especialmente en las *REDES SOCIALES*[68]*,* por parte de *MOVADEF*[69]*, EL*

---

[67] Ataque de Denegación de Servicios.- también llamado ataque **DoS** (siglas en inglés de *Denial of Service*) o **DDoS** (de *Distributed Denial of Service*), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

[68] Redes Sociales.- Es una estructura social compuesta por un conjunto de actores (tales como individuos u organizaciones) que están relacionados de acuerdo a algún criterio (relación profesional, amistad, parentesco, etc.). Normalmente se representan simbolizando los actores

MOVIMIENTO REVOLUCIONARIO TUPAC AMARU (MRTA) y SENDERO LUMINOSO (SL).

La pregunta que surge en esta etapa seria: *¿ ES ACASO LA APOLOGIA AL TERRISMO LA UNICA EXPERIENCIA QUE TIENE EL PERU DE UN SUPUESTO ATAQUE?* La respuesta es no, el Perú ha sido victimada de diverso ataques a entidades públicas, el problema es que no estamos preparados nisiquiera para diagnosticar en que momento estamos frente a un ciberataque.

Para desarrollar este punto previamente tenemos que comentar sobre un grupo de *HACKTIVISTAS*[70] llamado *ANONYMOUS.*

1. ANONYMOUS
    - Es un grupo que hace noticia cada día más en la red. Vestidos con máscaras blancas y bigote, con un expresión de sonrisa, la referencia más cercana la podremos encontrar en el personaje de cine y comic "V for Vendetta[71]".

    - ANONYMOUS es el seudónimo que utilizan varios individuos para realizar cierto tipo de acciones en la red, según el experto en *Ciber Seguridad* DAVID SANTIVAÑEZ, "ANONYMOUS justifica sus acciones en protesta a favor de la libertad de expresión, de

como nodos y las relaciones como líneas que los unen. El tipo de conexión representable en una red social es una relación diádica o lazo interpersonal.

[69] MOVADEF.- El Movimiento por la Amnistía y Derechos Fundamentales pretendió en el 2011 inscribirse como partido político ante el Jurado Nacional de Elecciones (JNE), pero su pedido fue rechazado, pues el grupo, fundado el 20 de noviembre del 2009, se basaba en el principio del "marxismo-leninismo-maoismo pensamiento 'Gonzalo'" y planteaba la amnistía general para los miembros de SL, ellos su líder máximo, Abimael Guzmán.

[70] Hacktivista.- Se entiende normalmente la utilización no-violenta de herramientas digitales ilegales o legalmente ambiguas persiguiendo fines políticos. Estas herramientas incluyen desfiguraciones de webs, redirecciones, ataques de denegación de servicio, robo de información, parodias de sitios web, sustituciones virtuales, sabotajes virtuales y desarrollo de software.

[71] V for Vendetta, o V de Venganza, como fue conocido en algunos países de Latinoamérica, es una seria de comics escritos por Alan Moore e ilustrados por David Lloyd. El argumento está situado en un futuro distopico ambientada en Gran Bretaña durante un futuro cercano, a finales de la década de los 90, y tras una guerra nuclear parcial, que ocasiono la destrucción de gran parte del mundo. Según nos va relatando la historia, un partido fascista ostenta el poder en el Reino Unido, y es un misterioso revolucionario apodado "V", oculto tras una máscara de Guy Fawkes, conspirador católico que, según la historia, planeo la Conspiración de la pólvora, cuyo objetivo era derribar el parlamento con explosivos situados en las bases del edificio y asesinar al Rey Jacobo I de Inglaterra, a sus familiares y al resto de la Cámara de los Lores, quien inicia una elaborada y violenta campaña con el fin de derrocar al gobierno e incitar a la población a adoptar un modelo político-social diferente.

la independencia de Internet y en contra de diversas organizaciones, como *SCIENTOLOGY, servicios públicos, consorcios con presencia global y sociedades de derecho de autor"*[72].

- Así mismo precisa SANTIVAÑEZ "Entre sus diversas actividades cuentan las manifestaciones en las calles y los ataques de hackers".[73]

Ahora que existe una idea clara de lo que *ANONYMOUS* es, plantearnos la siguiente pregunta debemos: *¿ES ANONYMOUS UNA AMENAZA?* Las actividades de *ANONYMOUS* no podemos calificarlas como amenazas, si bien *ANONYMOUS* son un grupo de hackers que tienen como misión informar de las informalidades que pretenden ocultar algunas empresa o entidades públicas, el ataque que realizan es a través de sus sistemas informáticos quebrando su seguridad a través de posibles vulnerabilidades a sus sistemas, sin cobrar ninguna víctima física o afectado servicios básicos como agua, luz o medios de comunicación.

Consideramos pertinente realizar un repaso por la actividad de *ANONYMOUS*, mencionando sus principales acciones, para así aclarar aún más la peculiar forma de actuar que tiene este grupo de hackers.

- ✓ **"The Internet Strikes Back" – "Internet Contra ataca".-** Fue una operación que el colectivo dirigió contra los sitio de instituciones ligadas a la página que facilitaba compartir archivos "Megauploud".[74]

- ✓ **"Redadas en Habbo".-** Es una red social diseñada como un hotel virtual, la primera intervención se debió a que un niño fue

[72] SANTIVAÑEZ ANTUNEZ, David Alonso. El delito de terrorismo informático como figura jurídica en el código penal peruano vigente: propuesta para su inclusión en la ley sobre delitos informáticos en el Perú, Tesis para optar el Título de Abogado, Universidad de Lima, 2014.
[73] Loc. Cit.
[74] RPP.COM.PE – Portal digital de RPP "Recuerde los ataques informáticos más importantes de Anonymous". Publicado 19 de Enero de 2012. En: http://rpp.pe/tecnologia/mas-tecnologia/recuerde-los-ataques-informaticos-mas-importantes-de-anonymous-noticia-442572 Información sustraída: 03/03/2016

impedido de ingresar a la piscina de un hotel en Alabama por tener SIDA.[75]

- ✓ **"Arresto de Chris Forcand".-** En diciembre de 2007 se realizó la detención del "Pederasta" *Chris Forcand,* luego que un grupo de vigilantes de internet "Anonymous" vigilara los movimiento en internet del hombre de 53 años.[76]

- ✓ **"Proyecto Chanology".-** El video de una entrevista a *Tom Cruise* producido por la *Iglesia de la Cienciología*[77] que llego a *Youtube*[78] en enero de 2008, causó el reclamo de la institución por la supuesta violación del *Copuright.*[79]

  En respuesta, *ANONYMOUS* lanzo el *El Proyecto Chanology* al considerar que las acciones de la Iglesia atentaban contra la libertad de expresión.[80]

- ✓ **"YouTube Porn Day".-** Integrantes de *ANONYMOUS* subieron videos *PORNOGAFICOS*[81] a *YOUTUBE* en protesta por la eliminación de videos musicales, los *HACKERS* disfrazaron el

[75] RPP.COM.PE – Portal digital de RPP "Recuerde los ataques informáticos más importantes de Anonymous". Publicado 19 de Enero de 2012. En: http://rpp.pe/tecnologia/mas-tecnologia/recuerde-los-ataques-informaticos-mas-importantes-de-anonymous-noticia-442572 Información sustraída: 03/03/2016

[76] RPP.COM.PE – Portal digital de RPP "Recuerde los ataques informáticos más importantes de Anonymous". Publicado 19 de Enero de 2012. En: http://rpp.pe/tecnologia/mas-tecnologia/recuerde-los-ataques-informaticos-mas-importantes-de-anonymous-noticia-442572 Información sustraída: 03/03/2016

[77] Iglesia de la Cienciología.- Es una secta devota a la práctica y promoción del sistema de creencias de la Cienciología. Fue fundada en diciembre de 1953 en Camden (Nueva Jersey) por el autor estadounidense de ciencia ficción L. Ron Hubbard (1911-1986). Su sede mundial se encuentra en Base Dorada, un área no incorporada del condado de Riverside, California.

[78] Youtube.- es un sitio web en el cual los usuarios pueden subir y compartir vídeos. Aloja una variedad de clips de películas, programas de televisión y vídeos musicales, así como contenidos amateur como videoblogs.

[79] Copyright.- es un conjunto de normas jurídicas y principios que afirman los derechos morales y patrimoniales que la ley concede a los autores.

[80] RPP.COM.PE – Portal digital de RPP "Recuerde los ataques informáticos más importantes de Anonymous". Publicado 19 de Enero de 2012. En: http://rpp.pe/tecnologia/mas-tecnologia/recuerde-los-ataques-informaticos-mas-importantes-de-anonymous-noticia-442572

[81] Pornografía.- hace referencia a todo aquel material que representa actos sexuales o actos eróticos con el fin de provocar la excitación sexual del receptor.

material como contenido para niños usando LINK[82] como *JONAS BROTHERS*[83].

- ✓ **"Gene Simmons".-** En 2010 el miembro de la banda *KISS*[84] pidió a las autoridades que fueran más agresivas ante las infracciones al *COPYRIGHT*, como respuesta a ellos *ANONYMOUS,* a través de la *OPERACIÓN PAYBACK* dejo fuera de servicio por más de un días los dos sitios del músico. [85]

- ✓ **"WikiLeaks".-** *ANONYMOUS* anuncia su apoyo a la página de *JULIAN ASSANGE*[86], lanzando ataques contra *AMASON*[87], *PAYPAL*[88], *MASTERCARD*[89], *VISA*[90] y el banco suizo *POSTFINANCE.* El apoyo de *ANONYMOUS* se debió a las presiones que sufría *WIKILEAKS* por la filtración de documentos diplomáticos.[91]

- ✓ **"Ataques contra la Ley Sinde en España"** .- En Diciembre del 2010 *ANONYMOUS* inició un ataque masivo contra las webs del Partido Socialista Obrero Español, Sociedad Generales de Autores de España, Congreso y Ministerio Cultura, esto debido a

---

[82] Link.- Hace referencia a una dirección de internet especifica.
[83] RPP.COM.PE – Portal digital de RPP "Recuerde los ataques informáticos más importantes de Anonymous". Publicado 19 de Enero de 2012. En: http://rpp.pe/tecnologia/mas-tecnologia/recuerde-los-ataques-informaticos-mas-importantes-de-anonymous-noticia-442572 Información sustraída: 03/03/2016
[84] KISS.- Banda de Musica Rock.
[85] RPP.COM.PE – Portal digital de RPP "Recuerde los ataques informáticos más importantes de Anonymous". Publicado 19 de Enero de 2012. En: http://rpp.pe/tecnologia/mas-tecnologia/recuerde-los-ataques-informaticos-mas-importantes-de-anonymous-noticia-442572. Información sustraída: 03/03/2016
[86] Julian Assange.- es un programador, ciberactivista, periodista y activista de Internet australiano, conocido por ser el fundador, editor y portavoz del sitio web WikiLeaks.
[87] Amazon.- Es una compañía estadounidense de comercio electrónico y servicios de computación en la nube a todos los niveles con sede en la ciudad estadounidense de Seattle, Estado de Washington.
[88] Paypal.- Es una empresa estadounidense fundada por Peter Thiel, Elon Musk y otros, pertenece al sector del comercio electrónico y permite pagar en sitios web, así como transferir dinero entre usuarios que tengan correo electrónico, una alternativa al convencional método en papel como los cheques o giros postales.
[89] Mastercard.- Es una marca de tarjetas de crédito y de débito.
[90] Visa.- Es una marca de tarjetas de crédito y de débito.
[91] RPP.COM.PE – Portal digital de RPP "Recuerde los ataques informáticos más importantes de Anonymous". Publicado 19 de Enero de 2012. En: http://rpp.pe/tecnologia/mas-tecnologia/recuerde-los-ataques-informaticos-mas-importantes-de-anonymous-noticia-442572. Información sustraída: 03/03/2016

promulgación que otorgaba pleno poder al Gobierno para cerrar paginas sin autorización de Juez.[92]

- ✓ **"Operación Tunisia".-** *ANONYMOUS* atacó en repetidas oportunidades paginas oficiales del Gobierno de Túnez, esto debido a la filtración de actos de corrupción por *WIKILEAKS.*[93]

- ✓ **"Protestas en Egipto en 2011"**.- *ANONYMOUS* ataca las páginas de *MINISTERIO DE INFORMACION* de *EGIPTO* y del *PARTIDO HOSNI MUBARAK*[94]*,* como apoyo a los manifestantes que pedían la admisión del *PRESIDENTE EGIPCIO.*[95]
- ✓ **"Operación Sony"**.- *ANONYMOUS* atacó los sitios web de *SONY* y del buffet de abogados que la representa, esto debido a que dos usuarios de PS3[96] filtraran datos.

Ahora que tenemos claro el tema con respecto a ANONYMOUS podemos continuar con el desarrollo de la investigación, para esto plantearemos la siguiente interrogante: ¿EL PERÚ HA SIDO VICTIMA DE ANONYMOUS? Como bien dice SANTIVAÑEZ, *"…su territorio es el mundo; mejor dicho el CIBERMUNDO…"*[97] no es posible determinar una nacionalidad al colectivo ANONYMOUS, es un grupo de especialistas en el campo digital, utilizando esta habilidad para alzar de protesta a través de la Internet.

---

[92] RPP.COM.PE – Portal digital de RPP "Recuerde los ataques informáticos más importantes de Anonymous". Publicado 19 de Enero de 2012. En: http://rpp.pe/tecnologia/mas-tecnologia/recuerde-los-ataques-informaticos-mas-importantes-de-anonymous-noticia-442572 Información sustraída: 03/03/2016

[93] RPP.COM.PE – Portal digital de RPP "Recuerde los ataques informáticos más importantes de Anonymous". Publicado 19 de Enero de 2012. En: http://rpp.pe/tecnologia/mas-tecnologia/recuerde-los-ataques-informaticos-mas-importantes-de-anonymous-noticia-442572 Información sustraída: 03/03/2016

[94] Hosni Mubarak.- Es un político y militar que ocupó el cargo de presidente de la República Árabe de Egipto.

[95] RPP.COM.PE – Portal digital de RPP "Recuerde los ataques informáticos más importantes de Anonymous". Publicado 19 de Enero de 2012. En: http://rpp.pe/tecnologia/mas-tecnologia/recuerde-los-ataques-informaticos-mas-importantes-de-anonymous-noticia-442572. Información sustraída: 03/03/2016

[96] PS3.- es la tercera videoconsola del modelo PlayStation de Sony Computer Entertainment. Forma parte de las videoconsolas de séptima generación y sus competidores son la Xbox 360 de Microsoft y la Wii de Nintendo.

[97] SANTIVAÑEZ ANTUNEZ, David Alonso. El delito de terrorismo informático como figura jurídica en el código penal peruano vigente: propuesta para su inclusión en la ley sobre delitos informáticos en el Perú, Tesis para optar el Título de Abogado, Universidad de Lima, 2014.

En cuanto al Perú, a pesar de no ser un país con el PBI[98] más elevado o con los índices de crecimiento tecnológico más elevados a nivel mundial, esto no evito que el Perú haya sido víctima de ANONYMOUS, según los reportes varios han sido los ataques sonados en las redes y medios de comunicación. Son los siguientes:

- ✓ "Anonymous atacó varios sitios web del Estado Peruano". Los sitios web de diversas páginas del Estado Peruano sufrieron esta tarde el ataque de Anonymous, un colectivo internacional integrado por hackers que ha atacado páginas de todo el mundo.[99] – Fecha 09 de Setiembre 2011.

- ✓ *"Anonymous filtra 1000 documentos del Gobierno Peruano". Como parte de la operación @OpCensorThis se publicaron los mencionados correos en donde se difunde el rol de entrega de valijas diplomáticas que se enviaron a Chile, Argentina, Ecuador, etc, desde nuestros país, se publicó también el nombre de los funcionarios responsables del cuidado de la valijas[100]. – Fecha 07 de Febrero de 2012.*

- ✓ "Anonymous ataca a la División de Delitos de Alta Tecnología de la DIRINCRI". Solo publica 200 correos personales[101]. - Fecha 04 de Marzo de 2012.

- ✓ "Anonymous Hackea a empresa de agua Sedalib". Ataque realizado en protesta por malos servicios y publicidad en burla

[98] PBI.- Sigla de Producto Bruto Interno.
[99] ELCOMERCIO.COM.PE – Portal digital de elcomercio "Anonymous atacó varios sitios web del Estado Peruano". Publicado 09 de Setiembre de 2011. En: http://elcomercio.pe/tecnologia/actualidad/anonymous-ataco-hoy-varios-sitios-web-estado-peruano-noticia-1284976 Información sustraída: 03/03/2016
[100] Peru21.pe – Portal digital del Diario Peru21. "Anonymous filtra 1000 documentos del gobierno peruano". Publicado el 07 de febrero de 2012. En: http;//peru21.pe/2012/02/07/actualidad/anonymous-filtra-mil-documentos-gobierno-peruano-2010892 Información sustraída: 06/03/2016
[101] PERU.com: "Anonymous publica casi 200 correos de Policía Informática" Publicado el 04 de Marzo de 2012. En: http://peru.com/2012/03/04/actualidad/nacionales/anonymous-publica-casi-200-correos-policia-informatica-noticia-45207 Información sustraída: 06/03/2016

de clientes por parte de esta compañía de agua[102]. - Fecha 08 de Julio de 2013.

- ✓ "Anonymous Perú Hackea web de entidades estatales". Se atacaron las webs de la Presidencia de la República del Perú, de la Región Lima, Huánuco y de las municipalidades de Carabayllo, Independencia y Ancón. #OperacionIndependencia[103]. - Fecha 28 de Julio de 2013.

- ✓ "Anonymous Perú Hackeo web de la Municipalidad de Lima". El servidor web de la comuna dejó de funcionar aproximadamente a las 11:00 p.m. Minutos después, Anonymous Perú escribió en Twitter[104] "Tango Down", una jerga militar que se utiliza cuando un enemigo ha sido abatido durante un conflicto. Pasadas las 7 a.m., el sitio web aún seguía inoperativo.[105] – Fecha 6 de Marzo 2015.

- ✓ "Reniec niega hackeo de su base de datos, pero Anonymous ratifica ataque". Después de que **Anonymous Perú** asegurara que vulneró la seguridad de los servidores del Registro Nacional de Identificación y Estado Civil (**Reniec**) y que se apropió de toda su base de datos, la institución descartó tal violación[106] - Fecha 13 de Marzo 2015.

---

[102] RPP.COM.PE – Portal digital de RPP Noticias. "La Libertad. Anonymous Hackea a empresa de agua Sedalib" Publicado el 08 de Julio de 2013. En: http://www.rpp.com.pe/2013-07-08-la-libertad-anonymous-hackea-a-empresa-de-agua-sedalib-noticia_611239.html Información sustraída: 06/03/2016

[103] CAPITAL.PE – Portal digital de Radio Capital. "Anonymous Perú hackea web de entidades estatales". Publicado el 28 de Julio de 2013. En: http://www.capital.com.pe/2013-07-28-anonymous-peru-hackea-web-de-entidades-estatales-noticia_617378.html

[104] Twitter.- Nombre de una Red Social. Información sustraída: 06/03/2016

[105] ELCOMERCIO.COM.PE – Portal digital de el Comercio "Twitter: Anonymous Perú hackeó web de la Municipalidad de Lima" Publicado el 06 de Marzo de 2015. En: http://elcomercio.pe/redes-sociales/twitter/twitter-anonymous-peru-hackeo-web-municipalidad-lima-noticia-1795706?ref=flujo_tags_223948&ft=nota_13&e=titulo Información sustraída: 06/03/2016

[106] LAPRENSA.PERU.COM - "Reniec niega hackeo de su base de datos, pero Anonymous ratifica ataque". Publicado el 13 de Marzo de 2015. En: http://laprensa.peru.com/actualidad/noticia-anoymous-peru-base-datos-reniec-niega-hacker-violacion-seguridad-40750

Es así como podemos apreciar que el Perú, no es ajeno a este tipo de incidentes, es a través de lo mostrado en la presente sección porque es importante tomar las recomendaciones dadas por las organizaciones internacionales y se demuestra porque es necesario la implementación de mejores mecanismos de control en nuestra realidad.

SEGUNDO CAPITULO
Ciber Soberanía

1. Nociones Generales acerca de la Soberanía Cibernética

a. Concepto

La presente investigación pretende vislumbrar las nuevas tendencias con respecto a la evolución del concepto de soberanía y su aplicación con las *Tecnologías de la Información y las Comunicaciones.*

El primer punto a tocar dentro de nuestra segunda sección será lo más básico, y lo desarrollaremos preguntándonos ¿QUE ES EL ESTADO? Consideramos necesario para responder la presente pregunta, debido a que, si bien la presente investigación no pretende desarrollar a profundidad temas de *TEORIA DEL ESTADO*, si consideramos necesario para definir que es *SOBERANIA*, establecer de manera clara quien o que la ejerce.

Entonces, para responder la pregunta plateada, utilizaremos el concepto de Vladimiro Naranjo Mesa, quien define al *ESTADO* de la siguiente manera: "*conglomerado social, política y jurídicamente organizado"*[107]*,* como podemos apreciar el concepto planteado por Naranjo es un concepto producto de varios cambios a lo largo de la historia, "para muestra un botón" el pensador Griego Protagoras nos dice "*el origen de los Estados fue una reunión de hombre, libres hasta ese momento*" el concepto de Protagoras aunque algo desmotivador tiene su base en la *TEORIA CONTRACTUALISTA,* tema que desarrollaremos más adelante, sobre el origen del *ESTADO*, y es pues a través de esta teoría que podemos entender porque Protagoras pensaba de esa forma.

Es necesario mencionar que el esfuerzo que pretendemos realizar al intentar definir al *ESTADO* es algo que mucho autores a lo largo de la historia han intentado, si bien todo forma parte de una evolución, no consideramos que

[107] NARANJO MESA Vladimiro (2014) "Teoría Constitucional e Instituciones Políticas", Colombia, Editorial Temis. Pp 217

los conceptos vertidos por diversos autores a lo largo de la historian sean malos o buenos, correctos o incorrectos; lo que buscamos es mostrar la evolución con respecto a la perspectiva de lo que estamos analizando, para ello nos muestran la evolución de la siguiente manera:

> *"Platón lo concibió como un ente ideal; Aristóteles como una sociedad perfecta; Hegel, Savigny y los románticos como un ser espiritual; Rousseau como la asociación política libremente fundada por los partícipes del contrato social; Kant como "reunión de hombre que viven bajo leyes jurídicas"; Kelsen lo identifica como una "ordenación de la conducta humana"; Carré de Malberg como un conjunto de elementos heterogéneos; Duguit los define como "una agrupación humana fijada sobre un territorio determinado, donde los más fuertes imponen su voluntad a los más débiles"; Burdeau como "titular abstracto y permanente del poder, cuyos gobernantes no son sino agentes de ejercicio esencialmente pasajeros"; Esmein como "la personificación jurídica de la Nacion"; Fischbach como "una situación de convivencia humana en la forma más elevada"; para Harold J. Laski, el Estado constituye una sociedad de hombres unidos por el deseo de enriquecer la vida colectiva. Del Vecchio lo define como "la unidad de un sistema jurídico que tiene en sí mismo el propio centro autónomo y que esta, en consecuencia, provisto de la suprema cualidad de persona en sentido jurídico".Biscaretti di Ruffia, por su parte, lo define como "ente social que se forma cuando en un territorio determinado se organiza jurídicamente en un pueblo que se somete a la voluntad de un gobierno". Para Marx es un instrumento de dominación de clases; para los anarquistas, en fin, es un obstáculo para la vida y la libertad del hombre. Bakunin decía que "el Estado es un inmenso cementerio donde vienen a enterrarse todas las manifestaciones de la vida individual". Lenin, por su parte, sostuvo que "ahí donde comienza el Estado termina la libertad". Mussolini, por el contrario, en el otro extremo,*

afirmaba que "el Estado es el absoluto delante del cual los individuos y los grupos no son sino lo relativo".[108]

Resulta evidente lo que Naranjo nos dice:

"De tal diversidad de definiciones y de enfoques, puede deducirse la extrema complejidad de la tarea de definir de manera certera la naturaleza de este ente."[109]

A pesar de la dificultad intentaremos acercarnos al concepto más actual utilizando las experiencias de diferentes autores dentro de la doctrina.

"…el Estado puede ser comprendido, en un sentido amplio mediante dos acepciones: como una estructura social y como una estructura de poder. En el primer sentido se toman en consideración los hechos que están en la base de su organización, primordialmente los hechos sociales, las relaciones humanas. En este sentido el Estado es objeto particular del estudio de la sociología y de la teoría general del Estado…En el segundo sentido, es decir como estructura de poder, se toman las relaciones de mando y obediencia existentes entre gobernantes y gobernados dentro del Estado, así como el vínculo jurídico que liga a todos sus componentes…"[110]

Para cerrar la idea de lo que es el Estado, debemos entender que el Estado como ente abstracto y como creación humana, ordena las relaciones que suscita en una realidad, utilizaremos una vez más lo que dice Naranjo:

"A)En sentido amplio, puede entenderse por Estado un conglomerado social, política y jurídicamente constituido, asentado sobre un territorio determinado, sometido a una autoridad que se ejerce a través de sus propios órganos, y cuya soberanía es reconocida por otros Estados. En este

[108] NARANJO MESA Vladimiro (2014) "Teoría Constitucional e Instituciones Políticas", Colombia, Editorial Temis. Pp 82
[109] Loc. Cit. Idem.
[110] Loc. Cit. Pp 84

sentido decimos, por ejemplo, que Colombia es un Estado, o que Francia es un Estado.

En la anterior definición encontramos los elementos constitutivos del Estado:

A) Un "conglomerado social, política y jurídicamente constituido", esto es la población; b) un territorio determinado, elemento físico; c) una autoridad que se ejerce a través de sus propios órganos", es decir, el poder público soberano; y d) el reconocimiento de la soberanía por otros Estados…

B) En Sentido restringido, la expresión Estado equivale, dentro de esa sociedad políticamente organizada, a los órganos que ejercen el poder público, esto es los gobernantes en sentido amplio, o sea quienes están investidos de autoridad sobre el conglomerado que forma la Nación. En este sentido se habla, por ejemplo, de un Estado intervencionista o de un Estado Absolutista.

C) En sentido más restringido, la palabra Estado se asimila dentro de la organización general de los poderes públicos, al poder central, del cual emanan las demás, directa o indirectamente. Se habla, entonces, de Estado central por oposición a las comunidades locales, a los departamentos, provincias, regiones, organismos descentralizados, etc."[111]

Así mismo el Dr. Brotons, establece que la Soberanía del Estado cuenta con 3 elementos:

***Territorio**: "espacio físico, terrestre, marítimo, aéreo, sobre el que se proyecta la soberanía o jurisdicción del Estado y en el que se ostenta el derecho exclusivo a ejercer sus funciones…"*[112]

[111] NARANJO MESA Vladimiro (2014) "Teoría Constitucional e Instituciones Políticas", Colombia, Editorial Temis. Pp 97

[112] BROTONS REMIRO, Antonio (1997) "Derecho Internacional", Madrid, Editorial Maite Vincueria Berdejo, Pp 44

> ***Población**: "…está compuesta esencialmente por nacionales del Estado…la nacionalidad es un estatuto muy privilegiado que se sustenta sobre la actividad laboral de mayorías extranjeras…la nacionalidad constituye un vínculo jurídico de los individuos con un Estado."*[113]

> ***Gobierno u Organización Política**: "…ha de entenderse la existencia de una organización política capaz de estableces y mantener el orden interno y pata para participar en la relaciones internacionales de forma independiente…"*[114]

Pero hablar de *ESTADO*, es hablar de dos escenarios, por una lado debemos entender que el *ESTADO* tiene una campo de acción interno, que es la relación entre el *SOBERANO* y *PUEBLO*; y por otro lado es necesario entender que el *ESTADO* también se relaciona con otro *ESTADOS* en un plano internacional, como bien nos dice Naranjo:

> *"De él surgían dos situaciones; las relaciones entre los individuos particulares, y las relaciones entre los Estados soberanos, surgidos del contrato. Los acuerdos de estas dos clases de partes contratantes daban origen al derecho interno, en el primer caso, y al derecho internacional, en el segundo, sujetos ambos a los principios del derecho natural. Las dos clases de derecho son, pues, producto de una pacto, y son obligatorias porque son impuestas por las partes que se obligan."*[115]

Entonces, ¿QUE ES EL ESTADO? Para responder la pregunta, utilizaremos a Hobbes, el cual nos dice en su obra celebre "Leviatán":

> "En efecto, gracias al arte se crea ese gran *Leviatán* que llamamos *república* o *Estado* (en latín civitas) que no es

[113] Loc. Cit. Pp 45
[114] BROTONS REMIRO, Antonio (1997) "Derecho Internacional", Madrid, Editorial Maite Vincueria Berdejo, Pp 46
[115] NARANJO MESA Vladimiro (2014) "Teoría Constitucional e Instituciones Políticas", Colombia, Editorial Temis. Pp 219

> sino un hombre artificial, aunque de mayor estatura y robustez que el natural para cuya protección y defensa fue instituido, y en el cual la *soberanía* es un alma artificial que da vida y movimiento al cuerpo entero; los *magistrados* y otros *funcionarios* de la judicatura y ejecución, nexos artificiales; la *recompensa* y el *castigo* (mediante los cuales cada nexo y miembro vinculado a la sede de la soberanía es inducido a ejecutar su deber) son los *nervios* que hacen lo mismo que el cuerpo natural; la *riqueza* y la *abundancia* de todos los miembros particulares constituyen su potencia; la *salus populi* (la salvación del pueblo) son sus negocios; los *consejeros*, que informan sobre cuantas cosas precisa conocer, son la *memoria;* la *equidad* y las *leyes*, una razón y una voluntad artificiales; la *concordia* es la salud, la sedición, la *enfermedad*; la guerra civil, la muerte. Por último, los *convenios* mediante los cuales las partes de este cuerpo político se crean, combinan y unen entre sí, aseméjanse a aquel *fiat*, o *hagamos al hombre,* pronunciado por Dios en la Creación"[116]

Sin duda, consideramos que la comparación entre el *ESTADO* y esta figura bíblica, es una de las más precisas para poder entender lo que es ésta creación humana, llamada *ESTADO.* Ahora bien, para resumir, *EL ESTADO ES UNA ENTELEQUIA CREADA POR EL HOMBRE QUE FORMABA PARTE DE UN TERRITORIO ESPECIFICO QUE BUSCABA ORGANIZAR LA VIDA EN SOCIEDAD Y LA SOBERANÍA, ORIGINARIAMENTE, ERA EL PODER DELEGADO DEL PUEBLO A UN SOBERANO.*

[116] HOBBES, T "Leviatán", I, Madrid, Ed. Sarpe, 1983, Introducción.

b. Origen del Estado - Teoría Contractualista

El origen del *ESTADO,* según algunos autores, como organización política se da a través de un *CONVENIO* o *PACTO SOCIAL,* y es según Naranjo*: "…ES ESTE EL QUE DA FUNDAMENTO A UNA AUTORIDAD LEGÍTIMA."*[117]

Según Naranjo:

> "*Quizá el primero en formular el concepto de "soberanía popular", con base en un contrato social, durante la Edad Media, fue el monje alemán Manegold de Lautenbach (siglo XI), quien enseño que el poder reside originariamente en el pueblo y el gobernante lo adquiere por un pacto social, y que si el monarca se convierte en tirano, infringe el pacto en cuya virtud fue elegido y puede ser destituido."*[118]

Sobre el *CONTRATO SOCIAL*, Locke nos dice:

> "*Siendo los hombres libres, iguales e independientes por naturaleza, ninguno de ellos puede ser arrancado de esa situación y sometido al poder político de otros sin que medie su propio consentimiento. Este se otorga mediante convenio hecho con otros hombres de juntarse e integrarse en una comunidad destinada a permitirles una vida cómoda, segura y pacífica de unos con otros, en el disfrute tranquilo de sus bienes propios, y una salvaguardia mayor contra cualquiera que no pertenezca a esa comunidad."*[119]

Como presupuesto, entonces para el *CONTRATO SOCIAL*, debe existir la libre voluntad del hombre para someterse al poder de su soberano, entiendo el término "hombre" como aquel grupo de personas que buscan organizar su vida en común.

Continúa Locke:

> "*Una vez que un determinado número de hombres ha consentido en constituir una comunidad o gobierno, quedan*

[117] NARANJO MESA Vladimiro (2014) "Teoría Constitucional e Instituciones Políticas", Colombia, Editorial Temis. Pp 217
[118] Loc. Cit. Idem.
[119] LOCKE, Jhon. Ensayos sobre el gobierno civil, Barcelona, Ediciones Orbis, S.A., 1983. Pp74

desde ese mismo momento integrados y forman un solo cuerpo político, dentro del cual la mayoría tiene el derecho de regir y obligar a todos. De esa manera todos cuantos consienten en formar un cuerpo político bajo un gobierno, aceptan ante todos los miembros de esa sociedad la obligación de someterse a la resolución de la mayoría, y dejarse guiar por ella: de otro modo, nada significaría el pacto inicial por el que cada uno de los miembros se integra con los demás dentro de la sociedad, y no existiría tal pacto si cada miembro siguiese siendo libre y sin más lazos que los que tenía cuando se encontraba en estado de naturaleza."[120]

El concepto de Locke sobre el *CONTRATO SOCIAL* es más político, debido a que él considera que la sociedad deberá ponerse de acuerdo para establecer al soberano que los va a guiar en donde la mayoría someterá a la minoría, y lo manifiesta en lo siguiente:

"*Tenemos, pues que lo que inicia y realmente constituye una sociedad política cualquiera, no es otra cosa que el consentimiento de un número cualquier de hombres libres capaces de formar mayoría para unirse e integrarse dentro de semejante sociedad. Y eso, y solamente eso, es lo que dio o podría dar principio a un gobierno legítimo."*[121]

Según Rousseau, el alejamiento del hombre a su "estado de naturaleza" hace que las organizaciones sean consideradas "intrínsecamente malas"[122] invocando a la violencia, en su obra *Discurso sobre la desigualdad entre los hombres*, en donde planteo la tesis que las organizaciones son basadas en la desigualdad, siendo la solución a este problema el *CONTRATO SOCIAL*.

[120] LOCKE, Jhon. Ensayos sobre el gobierno civil, Barcelona, Ediciones Orbis, S.A., 1983. Pp 74
[121] Loc. Cit. Idem.
[122] NARANJO MESA Vladimiro (2014) "Teoría Constitucional e Instituciones Políticas", Colombia, Editorial Temis. Pp 218

Para Rousseau el *CONTRATO SOCIAL* les da a las organizaciones la estabilidad e igualdad entre sus miembros como para poder continuar de manera armónica, él establece al *CONTRATO SOCIAL* de la siguiente manera:

> "*Las cláusulas de este contrato están de tal suerte determinadas por la naturaleza del acto, que la menor modificación en ellas las haría inútiles y sin efecto; de manera que, aunque no hayan sido jamás formalmente enunciadas, resultan en todas partes las mismas, así como tácitamente reconocidas y admitidas, hasta tanto que, violado el pacto social, cada cual recobra sus primitivos derecho y recupera su libertad natural al perder la condicional por la cual había renunciado a la primera."*[123]

Entonces es posible, que una de las partes viola el *CONTRATO SOCIAL* se puede volver al estado anterior? Naranjo, interpretando lo dicho por Rousseau, nos responde a la pregunta de la siguiente manera:

> "*…la vida social es más el fruto de un acuerdo voluntario establecido entre los hombres en determinado momento, que el resultado de una necesidad connatural al individuo. El contrato social es, pues, el resultado del acuerdo de voluntades, por medio del cual los hombres ponen en común ciertos intereses colectivos; pero si el contrato es violado, cada cual recobra la parte de libertad natural que ha sido alienada."*[124]

Una vez más Rousseau sobre el *CONTRATO SOCIAL:*

> *"Este acto de asociación transforma la persona particular de cada contratante en un ente normal y colectivo, compuesto de tantos miembros como votos tiene la asamblea, la cual recibe de este mismo acto su unidad, su vida y su voluntad. La persona pública que así se constituye, por la unión de todas las demás, tomaba en*

[123] ROUSSEAU, Jean-Jacques. El Contrato Social, Madrid, Ed. Sarpe, 1983, pp 41
[124] NARANJO MESA Vladimiro (2014) "Teoría Constitucional e Instituciones Políticas", Colombia, Editorial Temis. Pp 226

otro tiempo el nombre de ciudad y hoy el de Republica o cuerpo político, el cual es denominado Estado cuando es activo, potencia en relación con sus semejantes. En cuanto a los asociados, estos toman colectivamente el nombre de pueblo y particularmente el de ciudadanos, como participes de la autoridad soberana, y el de súbditos por estar sometidos a la leyes del Estado."[125]

La percepción de Rousseau del *CONTRATO SOCIAL* es la de un *ESTADO* como actualmente se le reconoce, la cual está compuesta por el mismo número de miembros como votos, para resumir la concepción roussoniana de la *SOBERANÍA* citaremos a Chevallier, que nos dice:

"*Los caracteres de la soberanía se desprenden lógicamente del origen contractual y de la definición del soberano. El soberano, constituido por el pacto social, es el pueblo como cuerpo decretando la voluntad general, cuya expresión es la ley. La voluntad del soberano es el soberano mismo. La soberanía, o poder del cuerpo político sobre todos sus miembros, se confunde con la voluntad general, y sus caracteres son los mismos de esta voluntad: es inalienable, indivisible, infalible, absoluta."*[126]

Continuando con el desarrollo del presente capitulo utilizaremos al profesor Maurice Hauriou y su *Teoría de la fundación y de la institución,* la cual nos explica lo siguiente:

"*El Estado aparece como una agrupación de individuos, dirigida por un gobierno central en nombre de una idea de fin, para la realización de un cierto orden social y político del que serán beneficiarios los súbditos del Estado. Este conjunto, formado por la idea de fin, el poder organizado para la realización de la idea y el grupo de individuos*

[125] ROUSSEAU, Jean-Jacques. El Contrato Social, Madrid, Ed. Sarpe, 1983, pp 43.
[126] CHEVALLIER, Jean-Jacques. Los grandes textos políticos, Madrid, Edit. Aguilar, 1981. Pp 153.

beneficiarios de dicho fin o proyecto, constituye esencialmente el organismo social estructurado."[127]

La teoría plateada por Hauriou, intenta quebrar la tesis planteada por Rousseau, ya que establece que para el nacimiento del *ESTADO* existe una voluntad común y no dos voluntades con intereses distintos, Naranjo nos lo explica:

"*Si analizamos la formación de estos organismos, vemos que aparecen elementos consensuales pero no elementos contractuales. El contrato se caracteriza esencialmente por un intercambio de consentimientos y de voluntades. En la compraventa, por ejemplo, el vendedor quiere ceder la cosa y recibir el precio, el comprador quiere pagar el precio y recibir la cosa. Cada una de estas voluntades, que se cruzan y se complementan, tienen un contenido y un objeto diferente. En la formación de un organismo colectivo no se da ese cruce de voluntades de contenido diferente. Todos los miembros de la agrupación desean y buscan la realización de la idea básica de asociación. En este caso, no nos hallamos en presencia de un cruce de voluntades, con contenido diferente, sino de un haz de voluntades con mismo contenido y tendente al mismo objeto. El error de Rousseau y de los sostenedores del contrato social y también del contrato político radica, como anota M. Hauriou, en creer que desde que aparecen elementos consensuales hay forzosamente contrato."*[128]

Con la tesis de Hauriou, separamos en dos momentos distintos al *CONTRATO SOCIAL*, si bien es necesario que exista la voluntad de ambas partes por crear una organización, es necesario también que se cree el documento físico y, evidentemente, que se aplique. Hauriou nos dice a través de Naranjo:

"Unos individuos conciben la idea de la empresa y los medios que se utilizaran para realizarla. Fundan un

[127] NARANJO MESA Vladimiro (2014) "Teoría Constitucional e Instituciones Políticas", Colombia, Editorial Temis. Pp 228
[128] NARANJO MESA Vladimiro (2014) "Teoría Constitucional e Instituciones Políticas", Colombia, Editorial Temis. Pp 229

> organismo por los procedimientos jurídicos que el ordenamiento vigente pone a su disposición. Reclutan, a continuación, adheridos para que les ayuden en la realización de su empresa. El grupo funciona entonces con este conjunto complejo: idea rectora, poder organizado, grupo de individuos interesados en la realización de la idea. Este conjunto constituye lo que se llama una institución."[129]

Si comprendemos el texto anterior, nos daremos cuenta que esa operación ocurre cotidianamente, no solo en caso de empresa, sino en caso de asociaciones e inclusive en la formación de *ESTADOS*, a lo cual Hauriou nos da un ejemplo:

> "*…la formación del Estado inglés y del Estado francés. El primero resulta de la fundación efectuada por el rey Guillermo el Conquistador y sus barones. La idea de empresa concebida por aquel es la conquista de un reino y su gobierno por procedimiento feudales ya utilizados en el continente. El poder organizado lo constituyen el rey Guillermo y sus barones, su ejército, sus consejeros. El grupo de interesados son las poblaciones inglesas, primero coaccionadas en cierta medida, luego verdaderamente interesadas por las ventajas de un régimen de Estado y obedientes a los mandamientos del poder real. La formación del Estado francés resulta igualmente de una fundación efectuada de común acuerdo por Hugo Capeto y los grandes feudatarios, que conciben las ventajas de un régimen político más centralizado, susceptible de desarrollar la cosa pública."*[130]

La relación que existe entre *CONTRATO SOCIAL, ESTADO Y SOBERANÍA*, es innegable, debido a que el *CONTRATO SOCIAL* es el acto por el cual el pueblo

[129] Loc. Cit. Ídem.
[130] NARANJO MESA Vladimiro (2014) "Teoría Constitucional e Instituciones Políticas", Colombia, Editorial Temis. Pp 229

acepta, en libre voluntad, someterse al *SOBERANO*, que a partir de ese momento, vendría a ser la entelequia llamada *ESTADO.*

c. Evolución de la soberanía

La palabra *Soberanía* proviene del latín *Super Amus* que significa *Señor Supremo*[131]*,* en donde desde el origen de las organizaciones políticas Griegas y Romanas, se asentaron los conceptos de poder supremo que la Organización ostentaba. Según el pensador Aristóteles:

> *"…la independencia potencial y…respeto exterior, independencia que se funda tal vez no tanto en su naturaleza de poder supremo, cuanto en la situación que le es propia al Estado de ser en sí mismo suficiente para satisfacer todas sus necesidades".*[132]

El concepto clásico de Soberanía, entendido desde la realidad Peruana, podría ser el que nos brinda el Dr. Brotons: "…el conjunto de competencias atribuidas al Estado por el Derecho Internacional ejercitables en un plano de independencia e igualdad respecto a los otros Estados."[133], desde este concepto podemos apreciar que la soberanía cuenta con un aspecto externo que es el reconocimiento de los demás estados.

Asi es confirma la idea de Brotons por Naranjo:

> *"...el poder del Estado tiene, entre otras características, el de ser soberano. Y esta soberanía atributo que habremos de examinar más adelante, se manifiesta de dos maneras: una interna, en cuanto se ejerce dentro del ámbito del Estado; y otra externa, cuanto que el Estado está colocado en pie de igualdad jurídica frente a los demás Estados que conforman la comunidad internacional."* [134]

---

[131] Informacion recogida de :http://etimologias.dechile.net/?soberani.a – 09/02/2016
[132] Georg Jellinek, Teoria General del Estado (Mexico: Fondo Cultural Económico, 2000), 402
[133] BROTONS REMIRO, Antonio (1997) "Derecho Internacional", Madrid, Editorial Maite Vincueria Berdejo, Pp 75
[134] NARANJO MESA Vladimiro (2014) "Teoría Constitucional e Instituciones Políticas", Colombia, Editorial Temis. Pp 144

Hablar de *SOBERANIA*, según el concepto mostrado, es hablar de la valides, aceptación o legitimidad que tenga el "*GOBERNANTE"* ante su pueblo, una vez más Naranjo nos dice:

> "El aspecto más importante de la doctrina de Althusius es el hecho de que hace residir la soberanía necesariamente en el pueblo como cuerpo, y, en consecuencia, es inalienable y no pasa jamás a manos de una familia o clase gobernante."[135]

Entonces, establecer a la *SOBERANÍA* como una constante inalienable, en la que el soberano detenta el poder, sería establecer que, en caso el pueblo deseara cambiar al soberano no podría? Para responder la pregunta Naranjo nos dice:

> *"El poder lo ejercen los funcionarios administrativos, que son investidos de él por las normas jurídicas del Estado, lo cual constituye, a su vez un segundo contrato, por el cual el cuerpo social imparte a sus administradores el poder necesario para llevar a la práctica sus propios fines. De ello se desprende que el poder revierte al pueblo, si quien lo detenta lo pierde por alguna razón…"*[136]

La *SOBERANIA* es el poder que el pueblo detenta y que requiere de una revalidación por parte de ambas partes, esto debido a que la relación que existe entre Gobernante y Gobernados es una relación que tiene como base el respeto a las condiciones establecidas en la constitución y establece los derechos, obligaciones y límites para ambas partes.

Una vez más Naranjo en su obra Teoría del Estado, nos recapitula algunos conceptos sobre soberanía:

> "*Para Burdeau "la soberanía es la cualidad de no depender de ningún orden político", y el soberano es el poder que impone "la idea de derecho" incorporada al Estado. Para Esmein, "la autoridad que naturalmente no reconoce*

[135] NARANJO MESA Vladimiro (2014) "Teoría Constitucional e Instituciones Políticas", Colombia, Editorial Temis. Pp 218

[136] SABINE, George H. "Historia de la Teoría Política", Mexico – Bogota, Fondo de Cultura Económica, 1976, pp 188.

potencia superior o concurrente en cuanto a las relaciones que ella rige, se llama la soberanía". Para Carre de Malberg, "la soberanía es el carácter supremo del poder: Supremo en cuanto a que ese poder no admite ningún otro por encima de él ni en concurrencia con él". Y agrega: "cuando se dice que el Estado es soberano, hay que entender por ello que en la esfera donde su autoridad es llamada a ejercerse él detenta una potencia que no surge de ningún otro poder y que no puede ser igualado por ningún otro poder"[137]

La evolución del concepto de *SOBERANIA* es un hecho podemos demostrar de manera expresa, en su origen, la *SOBERANIA* solo contaba con 3 elementos (Territorio, Población, Organización) pero con el desarrollo de las sociedades, estos 3 elementos fueron cambiando, ya no eran suficientes para reconocer al *ESTADO* que los 3 elemento converjan.

En primer punto, o dicho de otro forma el punto de origen de la *SOBERANIA* fueron los 3 elementos ya mencionados, pero que nos dice la historia con respecto a la *SOBERANIA*, es difícil considerar que en la época del *FEUDALISMO* existiera la *SOBERNIA* como actualmente la conocemos, Naranjo nos dice:

"La cuestión de la soberanía del Estado no se planteó en las antiguas organizaciones políticas orientales, ni entre los griegos o los romanos, aunque cabe recordar que fue en Roma donde primero se habló de superanitas para referirse a la autoridad suprema del emperadores. Tampoco significo gran cosa este concepto durante la Edad Media, cuando – como se vio – el poder de los monarcas, nominalmente soberanos, era disputado por los diversos estamentos, entre los que se destacaban las iglesias, los señores feudales, las municipalidades autónomas, los gremios, las ordenes de caballería y el Sacro Imperio Romano –

[137] NARANJO MESA Vladimiro (2014) "Teoría Constitucional e Instituciones Políticas", Colombia, Editorial Temis. Pp 236

Germánico, que aspiraba a imponerse universalmente y se resistió a reconocer la existencia de entidades territoriales autónomas."[138]

Entonces queda claro en qué momentos no se reconoció a la *SOBERANIA*, entonces a partir de qué momento en la historia podemos empezar a hablar de la *SOBERNIA* como actualmente la reconocemos? La *SOBERANIA* es productos de un desarrollo de la mentalidad colectiva humana, que lo que busco fue ordenar la vida en sociedad estableciendo un poder por encima de todo, así Naranjo nos da algún alcance de a partir de qué momento existió esta figura:

"El concepto moderno de soberanía nació de la lucha emprendida por la realeza – especialmente en Francia – para asegurar su independencia externa frente al Sacro Imperio y al Papado, y su supremacía interna frente a los señores feudales… Así el concepto de soberanía real aparece en sus orígenes como un arma forjada para sostener a la monarquía en su lucha para contrarrestar el poder del emperador, el papa y los señores"[139]

La soberanía es entonces el poder que ostenta el Estado dentro de un espacio determinado que emana del pueblo y es ejercido con respeto al ordenamiento jurídico, esto lo reconoce el Tribunal Constitucional Peruano como la *SOBERANÍA POLÍTICO – TERRITORIAL*, definiéndolo como:

"…el ejercicio del poder pleno, exclusivo y excluyente del que dispone un Estado sobre el territorio, pueblo y bienes materiales e inmateriales que se encuentran dentro de sus fronteras; derivándose de ello que, por sobre el orden jurídico nacional, no puede existir ni reconocerse voluntad ajena ni superior al Estado mismo, que interfiera en su propia organización política ni jurídica."[140].

[138] NARANJO MESA Vladimiro (2014) "Teoría Constitucional e Instituciones Políticas", Colombia, Editorial Temis. Pp 237
[139] Loc. Cit. Pp 238
[140] Tribunal Constitucional Perú - Expediente N.º 05761-2009-PHC/TC, fundamento 29.

El Tribunal Constitucional Peruanos, nos brinda el concepto actual de la magnitud del poder que ostenta el Estado, pero continuando con el devenir histórico, las diferentes formas de gobierno muestran la evolución de los criterios del hombre para ordenarse en grupos, así la evolución de la *SOBERANIA MONARQUICA* a la *SOBERNIA POPULAR*, fue un cambio no solo en conceptos sino también en la organización y forma de entender al gobierno o a la forma de gobierno.

> *"A partir del siglo XV, pero sobre todo a los largo del siglo XVI, se integraron y consolidaron los Estados nacionales en Europa. A ellos contribuyeron factores de diversa índole: sociológicos, como el despertar de la conciencia nacionalista; económicos, como el desarrollo del comercio exterior; intelectuales, como el Renacimiento y el redescubrimiento del Derecho romano; religiosos, como el desplazamiento de funciones de los estamentos feudales a manos de los reyes. Todos estos factores obraron en el sentido de atribuir al Estado un mayor ámbito de poder. Todo ello condujo a la instauración de una autoridad suprema, que de hecho poseía todos los poderes necesarios para el cumplimiento de su misión"*[141]

PERO EN QUÉ MOMENTO SE DIO EL CAMBIO ENTRE UNA Y OTRA? Naranjo lo aclara:

> *"Fue así como a partir de El contrato social, la teoría de la soberanía popular se convirtió en una bandera política que se enarbolo primero a raíz de la lucha por la emancipación de las colonias británicas de Norteamericana, luego en la Revolución francesa y después en las revoluciones de independencia de las antiguas colonias hispanoamericanas."*[142]

[141] NARANJO MESA Vladimiro (2014) "Teoría Constitucional e Instituciones Políticas", Colombia, Editorial Temis. Pp 247
[142] Loc. Cit. Pp 248

Así la teoría rousseauniana impacta en la evolución, no solo aportando conceptos a los orígenes del *ESTADO* sino también al concepto de *SOBERANIA*, en donde con su teoría del *CONTRATO SOCIAL* se da el impulso necesario para evolucionar los conceptos clásicos.

> *"…el concepto de soberanía popular se funda directamente sobre una confusión entre la soberanía estatal y la potestad del más alto órgano del Estado"*[143]

Después de la revolución francesa se deja de lado la teoría rousseauniana sobre *SOBERANIA,* dando paso a la *SOBERANIA NACIONAL,* Naranjo nos dice:

> *"…la soberanía popular fue modificada durante la Revolución francesa que consagro, el principio de la soberanía nacional, al designar al conjunto de los individuos, considerado como Nación, como titular de la soberanía."*[144]

El concepto queda ratificado y positivizado ya no solo a cargo de los diversos autores que ayudaron en el desarrollo del criterio de la civilización, así el artículo 3 de la Declaración de los Derecho del Hombre y del Ciudadano, establece:

> "El principio de toda Soberanía reside esencialmente en la Nación. Ningún cuerpo ni ningún individuo pueden ejercer autoridad alguna que no emane expresamente de ella."[145]

Queda claro entonces la idea de que la *SOBERANIA* no es divisible, no es posible fraccionarla en cada ciudadano, este nuevo concepto de *SOBERANIA*, que ya es generalizado y es aceptado por la comunidad Internacional, reconoce que ésta reposa en la totalidad de la Nación.

---

[143] CARRE DE MALBERG, René, Teoría general del Estado, Mexico, Fondo de Cultura Económica, 1948, pp 21.
[144] NARANJO MESA Vladimiro (2014) "Teoría Constitucional e Instituciones Políticas", Colombia, Editorial Temis. Pp 248
[145] Declaracion de los Derecho del Hombre y del Ciudadano, art. 3 - http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/espagnol/es_ddhc.pdf, información sustraída: 17/04/2016

Al respecto Naranjo nos dice:

> *"Muchos Estados en la era moderna han adoptado en sus constituciones el principio de la soberanía nacional, en tanto que otros han consagrado el de la soberanía popular. Aunque la adopción de uno y otro principio tiene implicaciones de orden práctico, como más adelante se verá, en la realidad, en la mayoría de los casos solo se trata de una distinción de tipo semántico, sin consecuencias materiales de trascendencia. Por ejemplo, en América Latina mientras algunas constituciones como la costarricense, la chilena o la uruguaya hablan de soberanía nacional, otras como la boliviana, la brasileña, la ecuatoriana, la mexicana o la peruana hablaron de soberanía popular; en realidad, todas ellas aplican – cuando en el respectivo país se practica la democracia representativa, naturalmente- , el principio de la soberanía nacional."*[146]

La pregunta que podríamos contestar después de aclarar el concepto de Soberanía seria: ¿EL ESTADO DEBE DEFENDER SU SOBERANÍA? Según el Tribunal Constitucional:

> *"…defender la soberanía nacional, garantizar la plena vigencia de los derechos humanos; proteger a la población de las amenazas contra su seguridad; y promover el bienestar general"*[147]

En nuestro ordenamiento jurídico, el Tribunal Constitucional a través de su jurisprudencia nos brinda parámetros al concepto de soberanía, como:

> "La soberanía emana del pueblo. Quienes lo ejercen lo hacen con las limitaciones y responsabilidades que la Constitución y las leyes establecen…"[148], complementando

[146] NARANJO MESA Vladimiro (2014) "Teoría Constitucional e Instituciones Políticas", Colombia, Editorial Temis. Pp 249
[147] Tribunal Constitucional Perú - STC 00001-2009-PI/TC, fundamento 134.
[148] Tribunal Constitucional Perú - Expediente Nº 05761-2009-PHC/TC, fundamento 28.

el concepto de soberanía de la siguiente forma: "…De ahí que la soberanía deba ser entendida como la potestad político-jurídica que permite decidir libremente sobre los asuntos internos y externos de un Estado…"[149]

Es evidente que de la relación existente entre el territorio con el estado y la población se tiene como resultado el poder llamado *SOBERANÍA* y para establecer los límites a este poder es necesario un documento que contenga los limites, las obligaciones y los derechos de quienes se encuentren dentro de la relación existente entre el *SOBERANO* y el *SUBDITO,* ese documento se llama *CONSTITUCIÓN*, y en el caso específico del PERÚ, la *CONSTITUCION POLITICA DEL PERÚ*, en ella se establece a través de su artículo 45:

"El poder del Estado emana del pueblo. Quienes lo ejercen lo hacen con las limitaciones y responsabilidades que la Constitución y las leyes establecen. Ninguna persona, organización, Fuerza Armada, Policía Nacional o sector de la población puede arrogarse el ejercicio de ese poder. Hacerlo constituye rebelión o sedición."*[150]*

Es así que la Constitución reconoce que el poder soberano proviene del pueblo para ser ejercido por las autoridades dentro de un marco normativo que sea de respeto al Estado Constitucional de Derecho y de los Derecho Humanos.

La experiencia Francesa a través de su *LIBRO BLANCO*, nos establece la relación que existe entre *ESTADO* y *SOBERANÍA:*

"La souveraineté repose sur l'autonomie de décision et d'action de l'État. Dans un monde interdépendant, elle n'est effective que si la Nation conserve la capacité de peser sur un environnement extérieur dont elle ne peut s'isoler.

Mais la Nation ne concourt durablement à la sécurité internationale que si les actions entreprises sont

[149] Loc. Cit. Ídem.
[150] Constitución Política del Perú, articulo 45.

reconnues comme légitimes. Le respect de l'État de droit renforce la souveraineté des États. La France entend préserver sa souveraineté, en se donnant les moyens de l'action et de l'influence, et contribuer à la sécurité internationale en inscrivant ses actions dans une légitimité nationale et internationale. Souveraineté et légitimité internationale sont donc deux fondements essentiels et complémentaires de sa stratégie de défense et de sécurité nationale."[151]

"La soberanía reside en la autonomía de decisión y la acción del Estado. En un mundo interdependiente, sólo es eficaz si mantiene la nación la capacidad de influir en el entorno externo en el que puede aislarse. Pero la nación se forma sostenible si contribuye a la seguridad internacional si las acciones se reconocen como legítimas. El respeto al estado de derecho fortalece la soberanía. Francia tiene la intención de preservar la soberanía, proporcionando los medios de acción y de influencia, y contribuir a la seguridad internacional mediante el registro de sus acciones en una legitimidad nacional e internacional. La Soberanía y la legitimidad internacional son dos pilares esenciales y complementarios de su estrategia defensa y seguridad nacional."[152]

Se hace necesario comentar que Francia reconoce que la legitimidad internacional es un elemento necesario del Estado Soberano, con el devenir histórico podremos apreciar como las agrupaciones de Estados se han convertido en parte de la doctrina evolución de la Soberanía, esto debido a la necesidad de Estado nuevo a ser reconocido como tal frente a los demás Estados, dándose así una suerte de "requisitos de valides" para los Estados.

[151] LELIVREBLANCDELADEFENSEETSECURITE.GOUV.FR – Portal del Libro Blanco de Defensa y la Seguridad, http://www.livreblancdefenseetsecurite.gouv.fr/pdf/le_livre_blanc_de_la_defense_2013.pdf, pp.19, Información sustraída: 24/04/2016

[152] Google traductor – Del Francés al Español.

Así el *ESTADO* y la *SOBERANIA* encuentran su relación a través de la obligación que se genera el *ESTADO* para defenderla, es por ello que se hace necesario desarrollar las medidas necesarias para poder afrontar los riesgos que afectan en la actualidad, reconociendo como un nuevo espacio o campo de acción al *CIBERESPACIO*, en donde debido a la evolución del *SOBERNIA* ahora se debe entender que en el *CIBERESPACIO* se habla de la *CIBERSOBERANIA*, la experiencia Francesa continua, y la reconoce de la siguiente forma:

> *"Attribut essentiel de la Nation, la souveraineté est un fondement de la sécurité nationale."*[153]
>
> *"Atributo esencial de la nación, la soberanía es un fundamento de la seguridad Nacional."*[154]

Actualmente es necesario entender que cuando se habla de "proteger el territorio" se debe entender que los elementos a los que se refiere son los siguientes:

- Territorio
- Cielos
- Mar
- *Ciber Espacio*

De forma más precisa lo establece Francia:

> *"S'agissant de la protection du territoire national et des ressortissants français, les risques et les menaces pris en compte par la stratégie de défense et de sécurité nationale sont:*
>
> *- Les agressions par un autre État contre le territoire national;*
>
> *- Les attaques terroristes;*
>
> *- Les cyberattaques ;*

[153] LELIVREBLANCDELADEFENSEETSECURITE.GOUV.FR – Portal del Libro Blanco de Defensa y la Seguridad, http://www.livreblancdefenseetsecurite.gouv.fr/pdf/le_livre_blanc_de_la_defense_2013.pdf, pp.19, Información sustraída: 24/04/2016

[154] Google traductor – Del Francés al Español.

- Les atteintes au potentiel scientifique et technique;

- La criminalité organisée dans ses formes les plus graves;

- Les crises majeures résultant de risques naturels, sanitaires, technologiques, industriels, ou accidentels;

- Les attaques contre nos ressortissants à l'étranger.

La protection du territoire national, de la population qui y vit et de nos compatriotes qui se trouvent à l'étranger est une obligation incontournable et fondamentale de l'État. Il lui appartient également de garantir la continuité des fonctions essentielles de la Nation."[155]

"En cuanto a la protección del territorio nacional y de nacionalidad francesa, los riesgos y las amenazas abordadas por la estrategia de defensa y la seguridad nacional son:

- La agresión de un Estado contra el territorio;

- Los ataques terroristas;

- Los ataques cibernéticos;

- Violaciones del potencial científico y técnico;

- El crimen organizado en sus formas más severas;

- Las grandes crisis originadas por riesgos naturales, la salud, tecnológicos, industrial o accidental;

- Los ataques contra nuestros ciudadanos en el extranjero.

La protección del territorio nacional, las personas que viven allí y de nuestros compatriotas que están en el extranjero es un requisito esencial y básico del Estado. También es responsable de garantizar la continuidad de las funciones esencial para la nación."[156]

[155] LELIVREBLANCDELADEFENSEETSECURITE.GOUV.FR – Portal del Libro Blanco de Defensa y la Seguridad, http://www.livreblancdefenseetsecurite.gouv.fr/pdf/le_livre_blanc_de_la_defense_2013.pdf, pp.47, Información sustraída: 24/04/2016

[156] Google traductor – Del Francés al Español.

Es necesario reconocer a los *CIBERINCIDENTES* como amenazas a la *SOBERANÍA* por ende como amenazas al *ESTADO* con lo cual se estaría afectando a la *NACIÓN* por ende nos afecta a todos.

> *"L'importance nouvelle de la cybermenace implique de développer l'activité de renseignement dans ce domaine et les capacités techniques correspondantes. Cet effort a pour objet de nous permettre d'identifier l'origine des attaques, d'évaluer les capacités offensives des adversaires potentiels et de pouvoir ainsi les contrer. Les capacités d'identification et d'action offensive sont essentielles pour une riposte éventuelle et proportionnée à l'attaque."*[157]

> *"La nueva importancia de la amenaza cibernética involucra el desarrollo de la actividad la información en este campo y las capacidades técnicas pertinentes. Este esfuerzo está destinado a permitir identificar el origen de los ataques, evaluar las capacidades ofensivas de los potenciales adversarios y el poder mostrado. Las capacidades de identificación y acción ofensiva son esenciales para una posible respuesta proporcionada a la agresión."*[158]

Francia ya en el 2013 reconoce la importancia de fortalecer al *CIBERESPACIO*, evidentemente lo hacen a través de todo un sistema que ayude de manera progresiva a mejorar los estándares de protección en esta materia, definitivamente es necesario establecer políticas que ayuden al desarrollo de la *CIBERSEGURIDAD* y la *CIBERDEFENSA.*

---

[157] LELIVREBLANCDELADEFENSEETSECURITE.GOUV.FR – Portal del Libro Blanco de Defensa y la Seguridad, http://www.livreblancdefenseetsecurite.gouv.fr/pdf/le_livre_blanc_de_la_defense_2013.pdf, pp.73, Información sustraída: 24/04/2016

[158] Google traductor – Del Francés al Español.

Es entonces la doctrina clásica de la Soberanía la que establece los 4 requisitos, pero ocurre que en tiempos modernos a través del desarrollo de nuevas tecnologías la soberanía ha sufrido un cambio, un nuevo miembro se ha sumado a la familia de los requisitos o presupuestos de la soberanía, *El Ciber Espacio*. Este nuevo campo de acción, al igual que el *territorio, el pueblo, la organización política y el reconocimiento de la comunidad internacional de los Estados* debe ser defendido por el Estado.

d. El reconocimiento del Estado

La investigación pretende demostrar cómo es que la evolución de conceptos como *ESTADO* y *SOBERANIA,* nos llevan a lo que hoy conocemos como *CIBERSOBERANIA*, para ello es necesario agotar el camino hasta llegar a punto que nos interesa.

Es así que el reconocimiento del Estado, fue un punto de evolución, y esto debido a que los *ESTADOS* ya establecidos buscaban agruparse, ya sea como bloque bélico, o por beneficios económicos, sea cual sea la razón es gracias a estos intereses que por parte de los *ESTADOS* de agruparse entre sí que desarrolla el nuevo elemento para la *SOBERANIA* y es el Reconocimiento del Estado por la Comunidad Internacional.
Nos dice Naranjo:

> *"…se manifiesta de dos maneras: una interna, en cuanto se ejerce dentro del ámbito del Estado; y otra externa, en cuanto que el Estado está colocado en pie de igualdad jurídica frene a los demás Estados que conforman la comunidad internacional."*[159]

El reconocimiento entonces podría ser tomado como *AQUELLA CONDICION POR LA CUAL LA COMUNIDAD INTERNACIONAL, (ORGANISMOS, ENTIDADES DE DERECHO INTERNACIONAL, ESTADOS); RECONOCEN A UN ESTADO*

[159] NARANJO MESA Vladimiro (2014) "Teoría Constitucional e Instituciones Políticas", Colombia, Editorial Temis. Pp 144

COMO SU IGUAL O MIEMBRO DE LA COMUNIDAD[160]*,* al respecto Naranjo nos dice:

> *"El reconocimiento de un Estado es el acto por el cual los demás Estados Declaran que trataran a un conglomerado determinado como a un Estado y que le reconocerán la calidad de tal."* [161]

Al respecto Charles Rousseau, nos dice:

> *"Reconocer a un Estado es dar testimonio de su calidad de tal; es decir, declarar que determinada entidad política será tratada como un sujeto de derecho internacional, investido de plena capacidad jurídica"*[162]

Es necesario que actualmente reconozcamos que este cuarto elemento es una nueva característica para la constitución de un *ESTADO*, esto sin restarles importancia a los demás.

> *"La existencia de este cuarto elemento del Estado no ha sido considerada, en general, por los tratadistas de derecho constitucional. Ello se debe, quizás, a que solo hasta la época contemporánea, en virtud del desarrollo que ha tenido el derecho internacional público, y a la cada vez más estrecha interrelación entre los estados soberanos, ha cobrado real importancia…Sin embargo, los internacionalistas coinciden en señalarlo…"*[163]

Naranjo es claro en establecer que es debido a la gran importancia que la Comunidad Internacional ha cobrado en la realidad actual, que como requisito para los "Estados Nuevos" sea necesario que este bloque ya existente de Estados los reconozcan como su igual.

---

[160] Concepto del Tesista.
[161] NARANJO MESA Vladimiro (2014) "Teoría Constitucional e Instituciones Políticas", Colombia, Editorial Temis. Pp 145
[162] ROUSSEAU, Charles, Derecho Internacional Público, Barcelona, Edic. Ariel, 1957. Pp80
[163] NARANJO MESA Vladimiro (2014) "Teoría Constitucional e Instituciones Políticas", Colombia, Editorial Temis. Pp 145

Al respecto la Convención Panamericana sobre los Derecho y Deberes de los Estados, establece:

> *"Artículo 1.—El Estado como persona de Derecho Internacional debe reunir los siguientes requisitos:*
>
> 1. *Población permanente.*
> 2. *Territorio determinado.*
> 3. *Gobierno.*
> 4. *Capacidad de entrar en relaciones con los demás Estados."*[164]

Los *ESTADOS* ya reconocieron como elemento constitutivo, que el reconocimiento es necesario, y así lo demuestra el acuerdo internacional de 1933, y sin éste elemento, no podrían gozar de los beneficios inherentes al *ESTADO*, este acto supone dos consecuencias:

> *"a) que el nuevo Estado adquiere derecho frente a la comunidad internacional, como son los de concluir tratados, hacerse representar diplomáticamente ante los otro Estados y ante los organismos internacionales.; y*
>
> *b) el eventual principio de su responsabilidad internacional."*[165]

e. *CiberSoberanía*

Llegamos al último punto dentro de esta segunda sección, la cual ha tenido como objetivo brindar los conceptos necesarios con respecto a la relación entre los elementos que conforman al *ESTADO* y su evolución.

Consideramos que la *CIBERSOBERANIA* se encuentra dentro del elemento territorio, bien sabemos que se considera territorio al suelo, subsuelo, espacio aéreo y marítimo. Esta evolución ha dotado al territorio con un aspecto adicional, el campo *VIRTUAL.*

---

[164] Convención Panamericana sobre los Derecho y Deberes de los Estados 1933.
[165] NARANJO MESA Vladimiro (2014) "Teoría Constitucional e Instituciones Políticas", Colombia, Editorial Temis. Pp 145

La *CIBERSOBERANIA* es el nuevo ámbito al cual el *ESTADO* tiene que prestar atención, esto debido a que como demostraremos más adelante los daños y el impacto negativo que genera un incidente *CIBERNETICO,* generan un alto riesgo, no solo para seguridad estatal sino también para los *USUARIOS* que al final son los que mantienen la *INTERNET* en constante desarrollo.

Utilizaremos el discurso inaugural de la Conferencia Mundial de Internet, a cargo del Presidente de China **Xi Jinping**, el cual en materia de *CIBERSOBERANIA* dice:

> *"El principio de la igualdad soberana consagrado en la Carta de las Naciones Unidas es una de las normas básicas en las Relaciones Internacionales contemporáneas. Cubre todos los aspectos de las relaciones entre estados, incluyendo también el ciberespacio".*[166]

Continúa de la siguiente forma:

> *"Se debe respetar el derecho de cada país a elegir de forma independiente el modo en el que quiere desarrollar su ciberespacio específico, su modelo de regulación cibernética y garantizar una participación igualitaria en la gobernanza ciberespacio internacional".*[167]

Pero, ¿POR QUE SERIA NECESARIO PROTEGER LA CIBERSOBERANIA DE ALGUN ESTADO? Utilizaremos la experiencia de Austria para responder a la pregunta, ellos consideran que el Ciber espacio a generado muchas oportunidades tales como:

> *"**Information and communication space**: Cyber space makes it possible to disseminate and transmit different sets of data and information resources. It is growing at a rapid pace: worldwide every minute about 204 million e-mails are sent, more than two million Google searches are*

[166] REALINSTITUTOELCANO.ORG, Portal de el Cano - http://www.blog.rielcano.org/la-ciber-soberania-china/, información sustraída: 17/04/2016
[167] Loc. Cit.- http://www.blog.rielcano.org/la-ciber-soberania-china/, información sustraída: 17/04/2016

conducted, Facebook is logged in six million times and more than 70 new domains are registered.

***Space for social interaction**: Cyber space is a space of general social interaction which is used by people for socialising. Today there are more than two billion Internet users globally.*

***Economic and trade space:** Cyber space has developed into a market place of strategic importance in a relatively short period of time. Based on estimates, the global e-commerce volume could almost double between 2012 (US $ 572 billion) and 2014.*

***Space for political participation**: Cyber space has an impact on the relationship between the government and society. The state reaches the citizens through e-government, offering facilitated access to government services. Digital forms of interaction open up new opportunities for political participation and political expression. The prerequisite for achieving this goal is to guarantee all human rights – both in virtual space and offline.*

***Control space**: The role of cyber space as a control space is closely connected to its function as an information space. By using this control space, it is practically possible to monitor, operate and maintain all infrastructures of the transport, economic, industrial, health and educational sectors. Based on estimates, up to 50 billion devices will be able to communicate with one another ("Internet of Things") by 2020. It will therefore be all the more important to ensure the security of this communication."*[168]

[168] AUSTRIAN CYBER SECURITY STRATEGY, Viena 2013, pp. 6 - https://www.bka.gv.at/DocView.axd?CobId=50999, información sustraída: 30/04/2016.

*"**Espacio de la información y la comunicación**: el espacio cibernético permite difundir y transmitir diferentes conjuntos de datos y recursos de información. Está creciendo a un ritmo rápido: en todo el mundo cada minuto se envían unos 204 millones de e-mails, más de dos millones de búsquedas de Google se llevan a cabo, Facebook se registra en seis millones de veces y más de 70 nuevos dominios son registrado.*

***Espacio para la interacción social**: el espacio cibernético es un espacio de interacción social general que se utiliza por la gente para socializar. Hoy en día hay más de dos millones de usuarios de Internet en todo el mundo.*

El espacio económico y comercial: el espacio cibernético se ha convertido en un mercado de importancia estratégica en un período relativamente corto de tiempo. Sobre la base de las estimaciones, el volumen global de comercio electrónico casi podría duplicarse entre 2012 (decir US $ 572 mil millones) y 2014.

Espacio para la participación política: el espacio cibernético tiene un impacto sobre la relación entre el gobierno y la sociedad. El estado llega a los ciudadanos a través de la administración electrónica, la oferta facilitó el acceso a los servicios gubernamentales. Las formas digitales de interacción abren nuevas oportunidades para la participación política y la expresión política. El requisito previo para la consecución de este objetivo es para garantizar todos los derechos humanos - tanto en el espacio virtual y fuera de línea.

Espacio de control: El papel del espacio cibernético como un espacio de control está estrechamente relacionada con

> su función como un espacio de información. Mediante el uso de este espacio de control, es prácticamente posible monitorear, operar y mantener todas las infraestructuras del transporte, económico, industrial, salud y educación. Basado en estimaciones, hasta 50 millones de dispositivos serán capaces de comunicarse una con otra ("Internet de las cosas") para el año 2020. Es por lo tanto, será tanto más importante para garantizar la seguridad de esta comunicación."[169]

Para un país como Austria, reconoce al Ciber espacio como un campo en el cual el Estado se ve íntegramente relacionado y lo demuestra a través de su estrategia en Ciber seguridad. Es por ello que reconoce las oportunidades que los Estados tienen actualmente para brindar mejores servicios o para acercarse a la población a través del Ciber espacio.

Al reconocer las oportunidades, reconocen también los riesgos inherentes a esta actividad, reconociendo que las oportunidades también generan riesgos a la Ciber Soberanía.

> "Cyber space as well as the security and safety of people in cyber space are exposed to a number of risks and threats as cyber space is also a space of criminal misuse. These risks and threats range from operating errors to massive attacks by state and non-state actors using cyber space as a venue for their activities, which is not limited by national borders; military operations may also be behind these attacks... Cyber crime, identity fraud, cyber attacks or misuse of the Internet for extremist purposes are serious new challenges facing all the stakeholders affected, requiring broad cooperation of governmental and non-governmental bodies at national and international level."[170]

[169] Google traductor – Del Inglés al Español.
[170] AUSTRIAN CYBER SECURITY STRATEGY, Viena 2013, pp. 6 - https://www.bka.gv.at/DocView.axd?CobId=50999, información sustraída: 30/04/2016.

> *"El ciberespacio, así como la seguridad y la seguridad de las personas en el espacio cibernético están expuestos a una serie de los riesgos y amenazas, así como el ciberespacio es también un espacio de uso delictivo. Estos riesgos y amenazas son una gama de errores de operación a ataques masivos de los actores estatales y no estatales que utilizan el ciberespacio como sede de sus actividades, que no está limitado por las fronteras nacionales; operaciones militares también puede estar detrás de estos ataques...El crimen cibernético, el fraude de identidad, ataques cibernéticos o mal uso de la Internet con fines extremistas, son serios desafíos nuevos que se enfrentan todos los grupos de interés afectados, que requiere una amplia cooperación de los organismos gubernamentales y no gubernamentales a nivel nacional y a nivel internacional."*[171]

No es difícil apreciar como Austria reconoce una posible situación de peligro frente a su Estado, y esto con el solo hecho de estar sujetos a la alta conectividad que tiene su Estado con la Internet, como bien lo expresan a través de su estrategia, los riesgos son grandes y pueden tener camuflados ataques militares de otros Estados.

Entonces la relación entre la Ciber Soberanía y el Ciberespacio es intima, con esta experiencia se muestra que el Ciberespacio de un Estado se encuentra sujeto a un sin número de posibles riesgos que no responden a límites fronterizos.

Así mismo la OTAN a través de su Centro de Excelencia en Estonia, nos dice:

> "A State may exercise control over Cyber infrastructure and activities within sovereign territory"[172]

[171] Google traductor – Del Inglés al Español.
[172] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE. Cambridge University Press, pp. 15.

> "Un Estado puede ejercer control sobre la infraestructura cibernética y actividades dentro del territorio soberano"[173]

Entonces la soberanía de la que hablamos no va direccionada sobre el Ciber espacio, sino más bien va a la soberanía que ejerce el Estado sobre sus infraestructuras críticas, para sustentar este punto, tenemos al Centro de Excelencia:

> "This rule emphazises the fact that although no State may claim sovereignty over cyber space per se, State may exercise sovereign prerrogative over any cyber infrastructure located on their territory, as well as activities associated with that cyber infrastructure."[174]
>
> "Esta regla enfatiza en el hecho de que ningún Estado puede reclamar soberanía sobre el espacio cibernético, per se, pero puede ejercer el Estado soberano prerrogativa sobre cualquier infraestructura cibernética situadas en su territorio, así como las actividades relacionadas con la infraestructura cibernética."[175]

Entonces la evolución de la que hablamos sobre la Ciber Soberanía, no está relacionada a poder ejercer Soberanía sobre el Espacio Cibernético, lo que la evolución de la Soberanía nos muestra es el poder ejercer soberanía sobre las infraestructura cibernética que se encuentre dentro del territorio de algún Estado.

Para concluir, entonces la Ciber soberanía, es una cualidad que Estado ha adquirido debido al desarrollo de las TIC s, pero es una vez más, no le da las prerrogativas sobre el Ciber Espacio, si no sobre las Ciber Estructura que el Estado ostenta, esto hace necesario que los Estados deban defender su soberanía, esto debido a que las Infraestructuras Criticas son de vital importancia para ellos.

---

[173] Google traductor – Del Inglés al Español.
[174] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE. Cambridge University Press, pp. 16.
[175] Google traductor – Del Inglés al Español.

> "It is the soveraignity that the state enjoys over territory that gives it the right to control cyber infrastructure and cyber activities within its territory."[176]
>
> "El Estado goza de soberanía sobre el territorio que le da el derecho de controlar las Ciber infraestructuras y sus actividades dentro de sus territorios."[177]

Esto confirma nuestra idea de la Soberanía, no podemos hacer que el Estado la ejerza soberanía sobre el Ciber Espacio, continuando con la idea:

> "Sovereignty implies that a state may control access to it´s territory and generally enjoys, within the limits set by treaty and customary international law, the exclusive right to exercise jurisdiction and authority on it´s territory.
>
> A state´s sovereignty over cyber infrastructure within it´s territory has two consequences. First, that cyber infrastructure is subject to legal and regulatory control by the state. Second, the state´s territorial sovereignty protects such cyber infrastructure."[178]

> "La soberanía implica El Estado puede controlar el acceso a su territorio y disfruta generalmente, dentro de los límites establecidos por los tratados internacionales y el derecho consuetudinario, el derecho exclusivo de ejercer la jurisdicción y la autoridad en su territorio.
>
> La soberanía de un Estado sobre la infraestructura cibernética dentro de sus territorios tiene dos consecuencias. Primero, que la infraestructura cibernética está sujeta a control legal y reglamentaria por parte del Estado. En segundo lugar, la soberanía territorial del Estado protege dicha infraestructura cibernética."[179]

---

[176] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE. Cambridge University Press, pp. 18.
[177] Google traductor – Del Inglés al Español.
[178] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE. Cambridge University Press, pp. 16.
[179] Google traductor – Del Inglés al Español.

Pero qué ocurre si dicha infraestructura se encuentra dentro de una red mundial de telecomunicaciones, se podría preferir que la comunidad internacional se mantenga a pesar que la soberanía del Estado no se vea afectada? La OTAN nos responde esto de la siguiente manera:

> "In the cyber context, the principle of sovereignty allows a state to, inter alia, restrict o protect (in part or in whole) access to the internet, without prejudice to applicable international law, such as human rights or international telecommunication law. The fact that cyber infrastructure located in a given State´s territory is linked to the global telecommunications network cannot be interpreted as a waiver of it´s sovereignty rights over that infrastructure."[180]

> "En el contexto cibernético, el principio de la soberanía permite a un estado, entre otras cosas, restringir o proteger (en parte o en su totalidad) el acceso a Internet, sin perjuicio del derecho internacional aplicables, tales como los derechos humanos o del derecho internacional de telecomunicaciones. El hecho de que la infraestructura cibernética situada en el territorio de un estado dado este vinculada a la red mundial de telecomunicaciones, no puede interpretarse como una renuncia a los derechos de soberanía sobre ella es esa infraestructura."

Antes de cerrar la el capítulo estableceremos las diferencias entre el Ciber espacio y el espectro electromagnético, para ello comenzaremos reconociendo al espectro electromagnético como un recurso natural y como tal el Estado es Soberano sobre él, así lo establece el Tribunal Constitucional:

> *"El espectro radioeléctrico o electromagnético es un recurso natural por medio del cual pueden propagarse las ondas radioeléctricas sin guía artificial. Es una franja de espacio a*

[180] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE. Cambridge University Press, pp. 17.

través de la cual se desplazan las ondas electromagnéticas capaces de portar y transportar diversos mensajes sonoros o visuales, a corta y larga distancia. Es un recurso natural de dimensiones limitadas. En tanto tal, de conformidad con el artículo 66º de la Constitución, forma parte del patrimonio de la Nación y el Estado es soberano en su aprovechamiento, correspondiéndole a éste su gestión, planificación, administración y control, con arreglo a la Constitución, la ley y los principios generales del demanio."[181]

Entonces ya podemos establecer que por un lado el espectro electromagnético es un recurso natural mientras que el ciber espacio no es reconocido como un recurso natural como hemos podido apreciar con lo definido líneas arriba, ahora bien para poder definir al ciber espacio utilizaremos a España:

"Cyberspace, the name given to the global and dynamic domain composed of the infrastructures of information technology - including the Internet - networks and information and telecommunications systems, has blurred borders, involving their users in an unprecedented globalisation that provides new opportunities but also entails new challenges, risks and threats."[182]

"Ciberespacio, el nombre dado al dominio global y dinámico constituido por las infraestructuras de tecnología de la información - incluyendo Internet - redes y sistemas de información y telecomunicaciones, las fronteras se ha difuminado, con la participación de sus usuarios de una globalización sin precedentes que ofrece nuevas oportunidades pero también conlleva nuevos retos , riesgos y amenazas"[183]

[181] Tribunal Constitucional Perú - Expediente N.º 0003-2006-PI/TC, fundamento 3.1.
[182] NATO.INT - Portal de la OTAN - https://ccdcoe.org/cyber-definitions.html - sitio visitado 21/05/2016.
[183] Google traductor – Del Ingles al Español.

Con esta definición de los que es ciber espacio, podemos centrar la diferencia entre ambos, uno como recurso natural mientras que el otro es definido como un dominio global que forma parte de las tantas creaciones humanas. Ahora bien ambas trasmiten información pero no se les puede confundir ni mezclar.

Entonces con esto queda cerrada la idea este nuevo aspecto de Soberanía, así pues como los Estados pueden, en una determinada situación ejercer más control y hasta prohibir el acceso en sus fronteras, en el tema de la Ciber soberanía el Estado podrá ejercer las misma prerrogativas pero para hacerlo tendrá que contar con los equipos y las capacidades humanas necesarias.

TERCER CAPITULO
CIBER GUERRA

1. Ciber Guerra

Es de consideración del Tesista, que la presente investigación ahonde en un tema poco desarrollado en la realidad Peruana, para ello aclararemos conceptos como los de *GUERRA TOTAL, GUERRA ASIMETRICA Y CIBERGUERRA,* para posteriormente poder establecer, según la realidad actual, temas con respecto al desarrollo tecnológico, en que momento nos encontramos y como se debería afrontar las nuevas amenazas.

- ✓ Guerra Total

Para definirla tomaremos las palabras de Carl Schmitt: *"La llamada guerra total cancela la distinción entre combatientes y no combatientes y conoce, junto a la guerra militar, otra no militar (guerra económica, propagandista, etc.) como emanación de la hostilidad..."*[184], se entiende que es un plano distinto al que usualmente se llevaban a cabo las "Guerras", según las ideas de SCHMITT, actualmente es posible desarrollar una guerra sin combate o como el menciona en la misma obra: "*…la guerra se hace ahora en un plano nuevo, intensificado, como activación ya no solo militar de la hostilidad…"*[185], es entonces la "Guerra" una situación que puede tener o no hostilidades? Según SCHMITT, "*El carácter total consiste aquí en que ámbitos de la realidad de suyo no militares (economía, propaganda, energías psíquicas y morales de los que no combaten) se ven involucrados en la confrontación hostil.*"[186], entonces la *GUERRA TOTAL* supone que dentro de las hostilidades de una "Guerra", adicionalmente se desarrollen ataques no hostiles desde otros ámbitos, como ha dicho SCHMITT pudiendo ser: económico, propagandista, político, tecnológico.

De lo anterior dicho es posible preguntarnos lo siguiente: ¿La participación en una *GUERRA TOTAL* es siempre voluntaria? Según José Tomás Hidalgo, no, y hace mención a lo siguiente:

[184] SCHMITT, Carl. Der Begriff des Politischen (El concepto de los políticos). Berlin: s.n., 1932.
[185] Loc. Cit. idem.
[186] Loc. Cit. idem.

"...la guerra total abarca todos los ámbitos del Estado y cancela la distinción de combatiente y no combatiente porque todos los ciudadanos participan, voluntaria o involuntariamente, en el esfuerzo de guerra y todos sufren los efectos de la guerra."[187]

- ✓ Guerra Asimétrica

Para desarrollar el siguiente punto utilizaremos como referente para el análisis las palabras de Antonio Cabrerizo Calatrava, el cual realizó una ponencia acerca del *CONFLICTO ASIMÉTRICO,* el cual se llevó a cabo en el Congreso Nacional de Estudios de Seguridad en la Universidad de Granada:

"...el que se produce entre varios contendientes de capacidades militares normalmente distintas y con diferencias básicas en su modelo estratégico. Alguno de ellos buscará vencer utilizando el recurso militar de forma abierta en un espacio de tiempo y ligar determinados y ateniéndose a las restricciones legales y éticas tradicionales. Su oponente y oponentes tratarán de desgastar, debilitar y obtener ventajas actuando de forma no convencional mediante éxitos puntuales de gran trascendencia en la opinión pública, agotamiento de su adversario por prolongación del conflicto, recurso a métodos alejados de las leyes y usos de la guerra o empleo de armas de destrucción masiva."[188]

Es entonces una "Guerra" en la cual se utilizan métodos alternativos, que al igual que la *GUERRA TOTAL*, se utilizan métodos distintos a los hostiles.

[187] HIDALGO TARRERO, José Tomás. Monografías 137, Necesidad de una conciencia nacional de CIberseguridad. La Ciberdefensa: un reto prioritario. Pp. 36.
[188] CABRERIZO CALATRAVA, Antonio Jesús. El conflicto asimétrico. Universidad de Granada: I Congreso Nacional de Estudios de Seguridad, 2002.

Con respecto a lo dicho por CABRERIZO, la diferencia fundamental entre la *GUERRA TOTAL* y la *GUERRA ASIMETRICA*, radica en la actividad pasiva y activa del ataque, en donde, mientras que uno (GUERRA TOTAL) activamente atacan sin hostilidad directa, en el otro (GUERRA ASIMETRICA) lo que se busca es "*desgastar, debilitar y obtener ventajas de forma no convencional"*

¿Se podría tomar a la GUERRA ASIMETRICA como un complemento de la GUERRA TOTAL? Se desprende de lo señalado por CABRERIZO que sí, y adiciona: "*Todos ellos con el objetivo principal de influir en la opinión pública y en las decisiones políticas del adversario."*[189] , es entonces otra forma de *atacar sin atacar.*

Según Hidalgo, la GUERRA ASIMETRICA: "*…uno de los bandos se aparta del cumplimiento de las leyes y usos de la guerra, aunque exige a su oponente dicho cumplimiento; los medios usados por la parte "débil" son económicos porque no tiene la capacidad de obtener y emplear medios a la atura del oponente "fuerte."*[190]*,* es necesario entender que la GUERRA ASIMÉTRICA se da por las misma condiciones de los actores, pudiendo ser entre ESTADOS o entre el ESTADO y ORGANIZACIONES TERRORISTAS, ello es mencionado por dos coroneles del Ejercito Popular Chino, QIAO LIANG y WANG XIANGSUI, quienes hacen mención al termino *GUERRA SIN RESTRICCIONES*[191]*,* hacen referencia de manera insistente que a la situación en uno de los oponentes se aleja de las leyes y usos de la guerra haciendo uso de las *CIBERARMAS* y *SISTEMAS CRÍTICOS* del enemigo, no solo como parte de la GUERRA ASIMETRICA entre Estados sino también como parte de lo que llamamos terrorismo[192].

[189] Loc. Cit. idem.
[190] HIDALGO TARRERO, José Tomás. Monografías 137, Necesidad de una conciencia nacional de CIberseguridad. La Ciberdefensa: un reto prioritario. Pp. 36.
[191] LIANG, Qiao y XIANGSUI, Wang. Unrestricted Warfare (Guerra sin restricciones). Beijing: PLA Literature and Arts Publishing House, febrero de 1999.
[192] HIDALGO TARRERO, José Tomás. Monografías 137, Necesidad de una conciencia nacional de CIberseguridad. La Ciberdefensa: un reto prioritario. Pp. 37.

- ✓ Ciberguerra

Según HIDALGO, se trata de un PARADIGMA que cuenta con similitudes a las dos anteriores. Así HIDALGO fundamenta las similitudes en lo siguiente:

- ✓ *Los efectos pueden alcanzar a todos los ciudadanos, administraciones, instituciones y empresas del Estado aunque no estén conectados al ciberespacio (Paradigma de la Guerra Total).*[193]
- ✓ *Involucra, voluntaria o involuntariamente, a todos los ciudadanos, administraciones, instituciones y empresas del Estado (paradigma de la Guerra Asimétrica).*[194]
- ✓ *La relación entre eficacia y coste es muy alta, posiblemente la más alta, ya que puede inutilizar sistemas básicos y críticos de un país con un coste para el atacante extraordinariamente bajo (paradigma de la Guerra Asimétrica).*[195]
- ✓ *No necesita de una infraestructura grande y costosa como la industria de armamento clásico –terrestre, naval, aéreo, NBQR*[196] *(paradigma de la Guerra Asimétrica).*[197]
- ✓ *Solo necesita personas con muy buena formación en ingeniería informática y en psicología.*[198]
- ✓ *En la CIBERDEFENSA pasiva deben participar todos los ciudadanos, administraciones, instituciones y empresas del Estado, cada uno a su nivel y con sus medios (paradigma de la Guerra Total y de la Guerra Asimétrica).*[199]

[193] HIDALGO TARRERO, José Tomás. Monografías 137, Necesidad de una conciencia nacional de CIberseguridad. La Ciberdefensa: un reto prioritario. Pp. 37.
[194] Loc. Cit. idem.
[195] Loc. Cit. idem.
[196] Siglas de "Nuclear, Bacteriológico, Químico y Radiológico".
[197] HIDALGO TARRERO, José Tomás. Monografías 137, Necesidad de una conciencia nacional de CIberseguridad. La Ciberdefensa: un reto prioritario. Pp. 37.
[198] Loc. Cit. idem.
[199] Loc. Cit. idem.

- ✓ *La CIBERDEFENSA activa es, o debe ser, función exclusiva, a nivel dirección, del Gobierno de la Nación.*[200]
- ✓ *Es muy difícil probar fehacientemente la autoría de un ataque a menos que el atacante quiera que se sepa, lo que proporciona un nivel de anonimato muy grande y convierte a la CIBERGUERRA en una guerra pérfida (paradigma de la Guerra Asimétrica).*[201]

De los expresado por HIDALGO podríamos hacernos la pregunta: ¿LA CIBERGUERRA TIENE SIMILITUDES CON LA GUERRA TOTAL Y CON LA GUERRA ASIMETRICA Ó ES UNA MEZCLA DE AMBAS?

Definitivamente la *CIBERGUERRA* es una mezcla de ambas y que por las características mostradas, se convierte en un paradigma con rasgos muy peligroso para afrontar y presenta un desafío para países como el Perú, que como ya hemos visto, nos encontramos en una situación en la que podemos ser atacados por organizaciones como *ANONYMOUS* y generar grandes pérdidas, no humanas pero si económicas y *LO MAS IMPORTANTE LA PERDIDA EN LA CONFIANZA DE LOS USUARIOS*, que son al final de todo, los que hacen que la *INTERNET* se mantenga y de desarrolle.

Habiendo ya presentado el paradigma central, que presenta una situación en la cual el abanico de posibilidades con respecto a las características de las hostilidades se expande, seguiremos desarrollando la investigación introduciendo un tema que vendría a ser el posible remedio o una forma de mellar en la *CIBERGUERRA*, la *CIBERSEGURIDAD.*

[200] Loc. Cit. Pp. 38.
[201] Loc. Cit. idem.

2. Ciber Seguridad Conceptualización

La *CIBERSEGURIDAD* es un concepto nuevo y de necesaria aplicación en todo ámbito actual de la vida cotidiana, la vida laboral y con mucho mayor razón es necesario que las personas con conocimientos técnicos en la materia capaciten de forma apropiada a otras para así poder tener un mejor sistema de seguridad, recordando siempre que la *INTERNET* es un red de usuarios la cual se fortalecerá en la medida que los usuarios apliquemos cierto estándares de seguridad en nuestra forma de navegar en la red.

Pero, según lo ya expuesto líneas arriba, la *INTERNET* es parte del *CIBERESPACIO* y no es más que una red de intercambio de información, entonces para introducirnos en la *CIBERSEGURIDAD* es necesario saber qué es lo que protegemos, y es *INFORMACIÓN*, pero surgen dos aristas, por lado se encuentra la *SEGURIDAD INFORMATICA* y la *SEGURIDAD DE LA INFORMACIÓN*.

¿SEGURIDAD INFORMATICA, SEGURIDAD DE LA INFORMACIÓN?*¿SON LO MISMO?* Pues no. Mientras que la *SEGURIDAD INFORMÁTICA* responde a la seguridad que deben de tener los sistemas de información o sistemas informáticos, la *SEGURIDAD DE LA INFORMACION*, responde a la seguridad de los datos transmitidos.[202]

Es en este punto en el que podríamos definir una conclusión preliminar, como la siguiente: LA CIBERSOBERANIA TENDRIA SU CAMPO DE ACCION EN LA PROTECCION DE INFORMACIÓN SENSIBLE DEL ESTADO, PUDIENDO TENER COMO FUENTE A INFRAESTRUCTURAS CRITICAS O ATAQUES MASIVOS A PAGINAS DE SERVICIOS PUBLICOS QUE BUSQUEN INAHIBILITARLAS.

Continuando con el desarrollo de la *SECCION*, nos toca hablar de los *CIBER*ATAQUES, en donde debemos entender que en todos los casos afecta a la *CIBERSOBERANIA,* pero estos podrán ser afrontados por la

[202] HIDALGO TARRERO, José Tomás. Monografías 137, Necesidad de una conciencia nacional de CIberseguridad. La Ciberdefensa: un reto prioritario. Pp. 38.

CIBERSEGURIDAD o la *CIBERDEFENSA*, no de maneras excluyente una con otra, pero si dependerá de la magnitud del ataque la respuesta.

- ✓ ***CIBERATAQUES***

La revolución tecnológica que nos arroyó a partir de la creación de las *TIC´s*, creo formas de delitos alternativos a los acostumbrados *HURTOS*[203] o *ROBOS*[204], con lo que nos vimos envueltos en una realidad en la que es posible no saber el *donde, cuando, quien y como* el atacante nos sustrae algún bien o información del *CIBERESPACIO*.

Es necesario tener presente que por el hecho de no conocer el *donde, cuando, quien y como* debamos dejar de utilizar el *CIBERESPACIO* o la *INTERNET*, si bien nos encontramos muchas veces desprotegidos, esto no es razón para aislar una herramienta tan poderosa o para cohibirnos por el peligro latente en el que nos encontramos cuando estamos en red.

Para demostrar por qué no debemos alejarnos del ciberespacio, no encuentro un mejor ejemplo que el expuesto por Hidalgo Tarrero, quien toma como referencia la actividad humana de volar, el cual establece la siguiente similitud:

> *"¿Por qué la seguridad de vuelo puede ser un referente? Hay varias razones para ello, entre las cuales podemos citar las siguientes:*
>
> - ✓ *En primer lugar, las amenazas a la seguridad de vuelo son muchas, pero las tripulaciones son conscientes de ellas, las asumen y se preparan para el caso de que se materialicen.*

[203] Código Penal Peruano – Hurto Simple: " Artículo 185.**-** El que, para obtener provecho, se apodera ilegítimamente de un bien mueble, total o parcialmente ajeno, sustrayéndolo del lugar donde se encuentra, será reprimido con pena privativa de libertad no menor de uno ni mayor de tres años. Se equiparan a bien mueble la energía eléctrica, el gas, el agua y cualquier otra energía o elemento que tenga valor económico, así como el espectro electromagnético y también los recursos pesqueros objeto de un mecanismo de asignación de Límites Máximos de Captura por Embarcación.**"**

[204] Código Penal Peruano – Robo: "Artículo 188.**-** El que se apodera ilegítimamente de un bien mueble total o parcialmente ajeno, para aprovecharse de él, sustrayéndolo del lugar en que se encuentra, empleando violencia contra la persona o amenazándola con un peligro inminente para su vida o integridad física será reprimido con pena privativa de libertad no menor de tres ni mayor de ocho años.

- ✓ *En segundo lugar, todos los involucrados en la operación de las aeronaves están concienciados de su importancia en la seguridad de las mismas y se preparan para ello.*
- ✓ *En tercer lugar, existe una organización de seguridad de vuelo presente en las instituciones que operan aeronaves, empresas de aviación, centros de control, etc.*
- ✓ *En cuarto lugar, hay conciencia y cultura de seguridad de vuelo, que cubre todas las fases del vuelo desde antes incluso de que las tripulaciones suban a bordo. La cultura es no punitiva, excepto caso de delito o negligencia flagrante, y se anima a todos los involucrados a notificar los errores cometidos y las incidencias sufridas.*
- ✓ *Los pasajeros también son conscientes de las amenazas inherentes al vuelo y sus riesgos pero los asumen y contribuyen, mayoritariamente, de acuerdo con las instrucciones comunicadas por los tripulantes de cabina de pasajeros.*
- ✓ *Esta conciencia y la cultura creada por esa conciencia han conseguido que volar, una actividad a priori peligrosa, sea de las más seguras con una tasa de accidentes muy baja."*[205]

Entonces conscientes que en el ciberespacio nos encontramos frente a peligros reales, pero que dependerá de la cultura que generemos para poder hacer que posibles vulnerabilidades dentro de los sistemas; sea cada vez menor, tomando como ejemplo lo mencionado por Hidalgo con respecto a la comparación de volar con el navegar por el ciberespacio.

Volver al ciberespacio en una actividad segura será una tarea ardua, esto debido, comparando con la actividad de volar, a que cuando nos

[205] HIDALGO TARRERO, José Tomás. Monografías 137, Necesidad de una conciencia nacional de CIberseguridad. La Ciberdefensa: un reto prioritario. Pp. 41.

encontramos en un avion[206] percibimos a través de nuestros sentidos el posible peligro que implica el estar a una determinada distancia del suelo y el hecho de caer desde esa distancia tendría como resultado la muerte, fuera del tenebroso momento de la caída. Caso contrario en el ciberespacio nosotros no podemos percibir el peligro con nuestros sentidos salvo cuando el atacante publica fotos nuestras en internet o transfieren dinero de nuestras cuentas bancarias, por ejemplo. Esto hace que se haga más difícil la labor de hacer que las personas comprendan el significado de la ciberseguridad porque muchas veces uno confía en lo que encuentra en internet.

Para definir el punto ciberataques y mostrar los diversos tipos que existen, consideramos que es necesario dejar sentados algunos conceptos o definiciones previas, para ello utilizaremos el Convenio de Budapest, sobre ciberdelincuencia de 2001.

Así el artículo primero del *CONVENIO DE BUDAPEST* establece:

> *"Capítulo I . Terminología*
>
> *Artículo 1 – Definiciones*
>
> *A los efectos del presente Convenio:*
>
> a. *Por "sistema informático" se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa."*

[206]RAE.ES-Avión-Del fr. *avion,* yeste der. del lat. *avis* 'ave[1]'.
1. m. Aeronave más pesada que el aire, provista de alas, cuya sustentación yavance son c onsecuencia de la acción de uno o varios motores. - http://dle.rae.es/?id=4a5PEam|4a6XWdH información sustraída: 22/04/2016

b. Por "datos informáticos" se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función;

c. Por "proveedor de servicios" se entenderá:

i. Toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático, y

ii. Cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo;

d. Por "datos relativos al tráfico" se entenderá todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente."[207]

Es así que el CONVENIO DE BUDAPEST en su Título 2 tipifica los DELITOS INFORMÁTICOS.

Título 2. Delitos informáticos

Artículo 7. Falsificación informática.

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno, cuando se cometa de forma deliberada e

[207] CONVENIO DE BUDAPEST, Convenio sobre Ciberdelincuencia, Articulo I – 23/11/2001

ilegítima, la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos, con independencia de que los datos sean o no directamente legibles e inteligibles.

Cualquier Parte podrá exigir que exista una intención fraudulenta o una intención delictiva similar para que se considere que existe responsabilidad penal.

Artículo 8. Fraude informático.

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante:

a) Cualquier introducción, alteración, borrado o supresión de datos informáticos;

b) cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona.

Título 3. Delitos relacionados con el contenido

Artículo 9. Delitos relacionados con la pornografía infantil.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

a) La producción de pornografía infantil con vistas a su difusión por medio de un sistema informático;

b) la oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático;

c) la difusión o transmisión de pornografía infantil por medio de un sistema informático,

d) la adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona;

e) la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos.

2. A los efectos del anterior apartado 1, por «pornografía infantil» se entenderá todo material pornográfico que contenga la representación visual de:

a) Un menor comportándose de una forma sexualmente explícita;

b) una persona que parezca un menor comportándose de una forma sexualmente explícita;

c) imágenes realistas que representen a un menor comportándose de una forma sexualmente explícita.

3. A los efectos del anterior apartado 2, por «menor» se entenderá toda persona menor de dieciocho años.

No obstante, cualquier Parte podrá establecer un límite de edad inferior, que será como mínimo de dieciséis años.

5. *Cualquier Parte podrá reservarse el derecho a no aplicar, en todo o en parte, las letras d) y e) del apartado 1, y las letras b) y c) del apartado 2.*

Título 4. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

Artículo 10. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

1. *Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de la propiedad intelectual, según se definan en la legislación de dicha Parte, de conformidad con las obligaciones asumidas en aplicación del Acta de París[208] de 24 de julio de 1971 por la que se revisó el Convenio de Berna para la protección de las obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI[209] sobre la propiedad intelectual, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.*

2. *Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de los derechos afines definidas en la legislación de dicha Parte, de conformidad*

[208] CONVENIO DE BERNA PARA LA PROTECCIÓN DE LAS OBRAS LITERARIAS Y ARTISTICAS.
[209] El Tratado de la OMPI sobre Derecho de Autor (WCT) es un arreglo particular adoptado en virtud del Convenio de Berna que trata de la protección de las obras y los derechos de sus autores en el entorno digital. Además de los derechos reconocidos en el Convenio de Berna, se conceden determinados derechos económicos. El Tratado también se ocupa de dos objetos de protección por derecho de autor: i) los programas de computadora, con independencia de su modo o forma de expresión, y ii) las compilaciones de datos u otros materiales ("bases de datos"). – Información sustraída de: http://www.wipo.int/treaties/es/ip/wct/ - información sustraída: 22/04/2016

con las obligaciones que ésta haya asumido en aplicación de la Convención Internacional sobre la protección de los artistas intérpretes o ejecutantes, los productores de fonogramas y los organismos de radiodifusión (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre las obras de los intérpretes y ejecutantes y los fonogramas, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

3. *En circunstancias bien delimitadas, cualquier Parte podrá reservarse el derecho a no exigir responsabilidad penal en virtud de los apartados 1 y 2 del presente artículo, siempre que se disponga de otros recursos efectivos y que dicha reserva no vulnere las obligaciones internacionales que incumban a dicha Parte en aplicación de los instrumentos internacionales mencionados en los apartados 1 y 2 del presente artículo."*[210]

El Convenio de Budapest es una buena herramienta para poder conocer lo que la comunidad internacional reconoce como cibercrimenes, pero ahora utilizaremos a la *OEA* para conocer algunas figuras que han sido reconocidas por esta Organización.

- ✓ *SPEAR-PHISHING – Robo de identidad con objetivo especifico*[211]
- ✓ *MALWARE – Programa malicioso*[212]
- ✓ *RANSOMWARE – Secuestro informático.*[213]

[210] CONVENIO DE BUDAPEST, Convenio sobre Ciberdelincuencia, – 23/11/2001
[211] Es un correo electrónico diseñado con ingeniería social con el objeto de engañar a una persona o un pequeño grupo de personas y realizar un ataque dirigido
[212] Método reconocido por la OEA como el principal ataque desde principios de 2000, utilizado para robar información sensible o confidencial.
[213] el atacante se hace pasar por agentes de las fuerzas de seguridad local y así exigen el pago de una multa falsa, que suele oscilar entre USD 100 y 500, como condición para desbloquear una computadora que estaba supuestamente bloqueada, y que había sido usada por las autoridades durante una investigación.

- ✓ *WATERING HOLE – Ataque a página web*[214]
- ✓ *SCADA - Supervisory Control And Data Acquisition*[215]
- ✓ *APT – Advance Persistent Threats*[216]

Habiendo ya mostrado los tipos de *DELITOS* y *ACTIVIDADES* son consideradas delictivas, consideramos necesario dar mayores alcances sobre algunas de ellas, como por ejemplo sobre los *SISTEMAS SCADA.*

- ***SISTEMA SCADA***

Como hemos visto en la presentación de la figura, el *SISTEMA* SCADA son las siglas en ingles de Supervisión, Control y Adquisición de Datos, "es un software para ordenadores que permite controlar y supervisar procesos industriales a distancia. Facilita retroalimentación en tiempo real con los dispositivos de campo (sensores y actuadores), y controla el proceso automáticamente. Provee de toda la información que se genera en el proceso productivo (supervisión, control calidad, control de producción, almacenamiento de datos, etc.) y permite su gestión e intervención"[217].

Al parecer el sistema scada no es ningún malware o algún tipo de ataque tipo *PHISIHNG o WATERING HOLE*, *SCADA* en palabras del *FBI*: *"NOT THE ONLY CONCERN, BUT CERTAINLY A MAJOR WORRY…"*[218] *"NO LA UNICA PREOCUPACION, PERO SIN DUDA UNA PREOCUPACION MAYOR**…"***
ES ENTONCES UNA PREOCUPACION MAYOR? POR QUE? Si como hemos visto es un programa informático que es utilizado para supervisar y controlar proceso en determinadas empresas, ahora bien si este punto le agregamos que este programa informático se encuentra en casi la totalidad de servicios utilizados el día de hoy, el escenario definitivamente cambia.

---

[214] Requiere que los atacantes infiltren un sitio web legitimo visitado por sus víctimas, instales un código malicioso y luego esperen que estas víctimas caigan en la trampa
[215] SUPERVISIÓN, CONTROL Y ADQUISICIÓN DE DATOS.
[216] Amenazas Avanzadas Persistentes.
[217] WIKIPEDIA.ORG – Portal de Wikipedia, https://es.wikipedia.org/wiki/SCADA Información sustraída fecha: 12/03/16
[218] LEB.FBI.GOV – Portal del FBI "CYBER TERROR" - https://leb.fbi.gov/2011/november/cyber-terror, Información sustraída fecha: 12/03/2016

El *FBI* nos dice lo siguiente:

> *"SCADA SYSTEMS HAVE EXISTED SINCE THE 1960. IN THE EARLY DAYS, THEY WERE STAND-ALONE, AND FEW WERE NETWORKED. TODAY, VIRTUALLY ALL ARE ACCESSED VIA THE INTERNET. THIS MAY BE GREAT AS A COST-CUTTING MEASURE, BUT NOT FROM AN INFORMATION SECURITY PERSPECTIVE. QUIETLY AND WITHOUT FANFARE, SCADA SYSTEMS HAVE PROLIFERATED RAPIDLY—FOR STARTERS, IN THE ELECTRIC, OIL, AND GAS; WATER TREATMENT; WASTE MANAGEMENT; AND MARITIME, AIR, RAILROAD, AND AUTOMOBILE TRAFFIC CONTROL INDUSTRIES. SCADA SYSTEMS ALSO ARE EMBEDDED IN "TELEPHONE AND CELL PHONE NETWORKS, INCLUDING 911 EMERGENCY SERVICES."*[219]

> *"Los sistemas SCADA han existido desde la década de 1960. En los primeros días, eran independientes, y pocos estaban conectados en red. Hoy, prácticamente todos se accede a través de Internet. Esto puede ser bueno como medida de reducción de costos, pero no desde una perspectiva de seguridad de información. En silencio y sin hacer ruido, sistemas SCADA vienen proliferan rápidamente, para empezar, en la electricidad, petróleo y gas; tratamiento de aguas; gestión de residuos; Y marítimo, aéreo, ferrocarril, y el automóvil control de tráfico industrias. Sistemas SCADA también están incrustados en "teléfono y celular Networks, que incluye servicios de emergencia 911."*[220]

EN DEFINITIVA MIENTRAS MÁS CONECTADOS A LA RED NOS ENCONTREMOS, VAMOS A TENER MAYOR Y MEJORES POSIBILIDADES DE ACCESO, VAMOS A PODER ENVIAR Y RECIBIR INFORMACIÓN, REALIZAR

[219] LEB.FBI.GOV – Portal del FBI "CYBER TERROR" - https://leb.fbi.gov/2011/november/cyber-terror, Información sustraída fecha: 12/03/2016
[220] Google Traductor – Del Inglés al Español.

OPERACIÓN DE MANERA MÁS RÁPIDA Y SENCILLA, PERO NOS ENCONTRAREMOS MÁS VULNERABLES FRENTE A HACKERS O POSIBLES ATACANTES QUE BUSQUEN FILTRARSE EN NUESTROS SISTEMAS.

Las ventajas son muchas pero es responsabilidad de todos hacer que la red, la internet y el ciberespacio se vuelvan seguros, para que así siga evolucionando y mejorando a medida que la confianza en la red, la internet y el ciberespacio va creciendo.

Con ideas más claras sobre esta forma de ciberataque, continuaremos con lo que nos dice Trend Micro[221] acerca de los sistemas SCADA.

> *"As we've mentioned, SCADA systems can be found industrially in a range of manufacturing or production environments including power plants and refineries, or in infrastructure environments for example controlling oil or gas pipelines and electrical power transmission. SCADA is the name given to the centralised computer system which monitors the entire distributed environment of a power plant or oil refinery, for example. The actual control actions are carried out by the Remote Terminal Units (RTUs) or by Programmable Logic Controllers (PLCs), according to the instructions sent to them by the SCADA, and are usually related to the heating, ventilation, air-conditioning or energy consumption.*
> *As you can imagine, with such a broad range of potential uses, SCADA machinery can be found in both public and private sector owned plants, but with such a potentially vital role in the smooth operation of key processes and*

[221] TREND MICRO, Empresa dedicada al desarrollo de software de Ciber seguridad a nivel mundial, actualmente consultora de CiberSeguridad de la OEA.

industries, it is imperative they remain free from interference by cyber criminals."[222]

"Como ya hemos mencionado, los sistemas SCADA se pueden encontrar industrialmente en una gama de entornos de fabricación o producción, incluidas las plantas de energía y refinerías, o en entornos de infraestructura, por ejemplo, el control de oleoductos y gasoductos y transmisión de energía eléctrica. SCADA es el nombre dado al sistema informático centralizado que controla todo el entorno distribuido de una refinería de petróleo o de la planta de energía, por ejemplo. Las acciones de control reales se llevan a cabo por las Unidades Terminales Remotas (RTU) o por controladores lógicos programables (PLC), de acuerdo con las instrucciones enviadas a ellos por el SCADA, y por lo general están relacionados con la calefacción, ventilación, aire acondicionado o la energía consumo.

Como se puede imaginar, con una amplia gama de usos potenciales tales, maquinaria SCADA se puede encontrar tanto en las plantas del sector de propiedad pública y privada, pero con un papel potencialmente importante en el correcto desarrollo de los procesos y las industrias clave, es imperativo que se mantengan sin injerencia de los delincuentes cibernéticos."[223]

Una empresa como Trend Micro publica lo necesario acerca de las vulnerabilidades a los sistemas SCADA en el 2011, realizó todo un análisis preciso para la época en la que se publica el informe, éste continua con una pregunta, que a nuestro parece clave, es: *¿ARE SCADA SYSTEMS SAFE? - ¿SON SEGURO LOS SISTEMAS SCADA?* Esta es una pregunta que para la época en la que se publica el informe, era más que necesario entender:

---

222 TRENDMICRO.COM- Portal de Trend Micro**,** SCADA threats: a new front in the war against cyber crime? - http://blog.trendmicro.com/scada-threats-a-new-front-in-the-war-against-cyber-crime/ , Publicacion sustraída fecha: 13/03/16

223 Google Traductor – Del Inglés al Español.

"*It has long been suspected that these systems were lacking when it comes to security, but the discovery of 34 vulnerabilities by security researcher Luigi Auriemma, was still a massive blow to the makers of SCADA systems. It appears as if the manufacturers were relying too much on security by obscurity. This is the rationale that hackers would ignore such systems because they'd have to spend far too long researching the technology to generate a decent RoI. The vendors were also likely still in the mindset that many of the systems were not connected to the internet and therefore more secure, although increasingly SCADA systems are actually being networked because of the superior efficiency gains and improved manageability that can be achieved*."[224]

"*Durante mucho tiempo se ha sospechado que estos sistemas eran escasos cuando se trata de seguridad, pero el descubrimiento de 34 vulnerabilidades de seguridad por el investigador Luigi Auriemma, seguía siendo un duro golpe a los fabricantes de sistemas SCADA. Parece como si los fabricantes confiaban demasiado en la seguridad por oscuridad. Esta es la razón de que los hackers podrían ignorar este tipo de sistemas, ya que tendrían que pasar demasiado tiempo a investigar la tecnología para generar un ROI decente. Los vendedores también tendrían probablemente todavía el modo de pensar que muchos de los sistemas no estaban conectados a la Internet y por lo tanto eran más seguro, aunque cada vez más los sistemas SCADA, en realidad, se están conectados en red a causa*

224 TRENDMICRO.COM- Portal de Trend Micro**,** SCADA threats: a new front in the war against cyber crime? - http://blog.trendmicro.com/scada-threats-a-new-front-in-the-war-against-cyber-crime/ , Publicacion sustraída fecha: 13/03/16

de la mayor eficiencia y capacidad de gestión superiores que se puede lograr mejorar."[225]

La idea es clara, *A MENOR CONECCIÓN A LA INTERNET O A LA RED, MENOR ES EL RIESGO, O MENORES SERAN LAS VULNERABILIDADES,* con el desarrollo de las *TICs*, era inevitable que este tipo de sistemas evolucionen. Haciendo un símil, en la actualidad muchas personas pueden controlas las cámaras de seguridad de sus empresa u hogares, y muchas veces no solo tenemos interconectadas las cámaras sino también la alarma de seguridad y hasta los pestillos de acceso, esto lo hacen a través de la internet y gracias a la evolución de los dispositivos moviles que ayudan a que la seguridad de nuestros bienes la podamos llevar a todos sitios, esta ventaja genera una ventana de vulnerabilidades que pueden ser explotadas por ciberatacantes.
Pero que es lo que hace a los sistemas *SCADA* diferentes de otros sistemas? Para el investigador *Luigi Auriemma*[226]*,* la diferencia no existe, lo dice de la siguiente manera:

"In technical terms the SCADA software is just the same as any other software used everyday…"[227]

"En términos técnicos, el software SCADA es lo mismo que cualquier otro software que se utiliza todos los días".[228]

Es necesario que aclaremos la siguiente idea, si bien en el presente punto hemos vertido los conceptos de manera separa esto no quiere decir que para su aplicación no interactúen unos con otros, por ejemplo, el cibercriminal podrá logras su objetivo de entrar al sistema *SCADA* a través de un malware que es enviado a la víctima a través de un correo electrónico, o se instala un malware a través de una campaña de watering hole en una página, esto confirma la constante evolutiva que lleva a los ciberatacantes a desarrollar

[225] Google Traductor – Del Inglés al Español.
[226] Luigi Auriemma es el co-fundador y investigador de seguridad en ReVuln Ltd. Ha estado en el campo de la seguridad durante más de una década como un investigador de seguridad independiente. Descubrió más de 2000 vulnerabilidades en el software utilizado.
[227] TRENDMICRO.COM- Portal de Trend Micro**,** SCADA threats: a new front in the war against cyber crime? - http://blog.trendmicro.com/scada-threats-a-new-front-in-the-war-against-cyber-crime/ , Publicación sustraída fecha: 13/03/16
[228] Google Traductor – Del Inglés al Español.

nuevas formas que a través de *INGENIERIA SOCIAL*[229]o mecanismos que los ayuden a conseguir sus objetivos, *POR LO QUE ES IMPERATIVO QUE PARA HACER QUE LA REALIDAD JURÍDICA DE NUESTRO PAÍS CAMBIE Y LOGRE DESARROLLARSE A UN VELOCIDAD SUPERIOR A LA ACTUAL, QUE NO SE TIPIFIQUE EN BASE A LA ACCION O A LA CONDUCTA, SI NO EN BASE A LOS RESULTADOS QUE ESAS ACCIONES O CONDUCTAS PRODUCEN EN LA REALIDAD,* esto debido a que como ya se comentó, la conducta puede modificarse, y lo más probable es que se modifique o que evolucione con el tiempo, pero lo que no va a modificarse es el resultados.

Es inevitable recapacitar en que no solo se crean formas de ciberataques nuevas, si no también se crean nuevos objetos de ataques, como en su momento fueron los sistemas *SCADA*, ahora son los ataques a *CLOUDS*[230] o *NUBES,* así como los ataques a todos los dispositivos *SMART*[231] o dispositivos *INTELIGENTES.*

En la actualidad los dispositivos smart son cada vez más frecuentes, esta revolución comenzó con la aparición de los celulares[232] que poco a poco fueron tomando cierta importancia en el día a día de las personas por lo que fue necesario desarrollar la tecnología y hacer que la experiencia con los celulares se volvieran cada vez sencillas, tan es así que la empresas en un afán de facilitar a su consumidores las labores que se realizaban antes de manera presencial ahora se pueden desarrollar con tan solo presionar una tecla, esto como ya lo hemos visto genera mucha rapidez en el intercambio de datos y de información pero genera ventanas de posibles vulnerabilidades que, antes de ofrecer el servicio, se deben de proteger para evitar inconvenientes posteriores.

---

[229] La ingeniería social, un término creado por un hacker reconvertido a consultor, es el acto de engañar a la gente para que haga algo que no desea hacer o que proporcione información confidencial. Los *CIBERDELINCUENTES* se valen de esta popular herramienta para obtener beneficios y lucrarse económicamente.

[230] Permite una separación funcional entre los recursos que se utilizan y los recursos de tu computadora, esto es: *SE UTILIZAN RECURSOS EN UN LUGAR REMOTO Y QUE SE ACCEDEN POR INTERNET.*

[231] Un dispositivo *SMART O INTELIGENTE* es un dispositivo electrónico, por lo general conectado a otros dispositivos o redes, que puede funcionar hasta cierto punto de forma interactiva y autónoma.

[232] Un dispositivo electrónico para telecomunicaciones personales con red inalámbrica.

El hecho de ser smart no significa que sea seguro, al contrario, mientras más smart menos seguro será, si el proveedor del bien o servicio no toma las acciones pertinentes para ofrecer esos bienes o servicios de manera segura.

Esta revolución smart hace que cada vez más artefactos eléctricos de uso diario se conviertan, así pues, como ya mencionamos, comenzó con el celular, continuo con las tablets[233], con los relojes smart[234], automoviles smart[235] y así podemos llegar a las casa y edificios smart, esta evolución no llevara a que las ciudades dentro de poco se adquieran esta característica smart.

Como se puede apreciar la evolución nos muestra un futuro en el cual la todo se encontrara interconectado a la internet, haciendo que la vida cotidiana encuentre solución rápida a problemas diarios, esto gracias a la posibilidad de encontrarnos conectados a la internet.

Volviendo a los *CIBERATAQUES* existe un tipo de ataque que es conocido como *APT (Advanced Persistent Threat) (Amenaza Avanzada Persistente)* que según *TREND MICRO* es:

> *"refer to a category of threats that pertain to computer intrusions by threat actors that aggressively pursue and compromise chosen targets."*[236]
>
> *"Una categoría de amenazas que se refieren a las intrusiones informáticas por los agentes de amenaza que*

[233] Computadora portátil de mayor tamaño que un teléfono inteligente o un PDA(Asistente Personal Digital), integrada en una pantalla táctil (sencilla o multitáctil) con la que se interactúa primariamente con los dedos o un estilete (Instrumento de Escritura), sin necesidad de teclado físico ni ratón.

[234] Reloj de pulsera dotado con funcionalidades que van más allá de las de uno convencional. Los primeros modelos desempeñaban funcionalidades muy básicas, pero los actuales ya son capaces de acceder a internet, realizar y recibir llamadas telefónicas, enviar y recibir emails y SMS, recibir notificaciones del smartphone e incluso consultar las redes sociales. Muchas de las funcionalidades que integran ya están disponibles en los smartphones.

[235] Automóviles Smart son aquellos que cuentan con diversas funciones de conectividad que permiten que el conductor y que los pasajeros cuenten con una mejor experiencia en el viaje con respecto a las herramientas que pueden usar como son servicios de GPS, acceder a videos ONLINE, inclusive la posibilidad que el automóvil se estaciones de forma automática utilizando sensores.

[236] TRENDMICRO.COM- Portal de Trend Micro**,** GLOSARIO - http://www.trendmicro.com/vinfo/us/security/definition/apt-advanced-persistent-threat , Publicación sustraída fecha: 13/03/16

persiguen y comprometen blancos elegidos de manera agresiva."[237]

- ***APT – ADVANCED PERSISTENT THREATS***

Siguiendo con el desarrollo de ciberataques, el siguiente punto es una nueva amenaza a las infraestructuras críticas. Para explicar este nuevo tipo de amenaza Trend Micro, nos dice:

> *"Many people assume that the 'Advanced' in Advanced Persistent Threats means the use of some incredibly new sophisticated malware but typically that's not the case. Usually the 'Advanced' element is in the research effort and the social engineering to tip a specific target over the edge and get them to click though to a URL of the attackers choosing."*[238]
>
> *"Mucha gente asume que lo de 'avanzada', en persistentes amenazas avanzadas significa que el uso de algún nuevo malware sofisticado, pero por lo general eso no es el caso. Por lo general, el elemento "Avanzado" está en el esfuerzo de investigación y la ingeniería social para inclinar a un objetivo específico sobre el borde y conseguir que se haga clic a una dirección URL*[239] *de la elección de los atacantes."*[240]

Según Trend Micro no es un ataque especial, tampoco cuenta con una tecnología avanzada que haga de este un ataque peligroso, lo que si utiliza es mucho más tiempo para poder ubicar las vulnerabilidades dentro de un ordenador y así poder extraer la información que busca, como se puede

---

[237] Google Traductor – Del Inglés al Español.

[238] TRENDMICRO.COM- Portal de Trend Micro**,** Cloud Security and APT defense – Identical Twins? http://blog.trendmicro.com/cloud-security-and-apt-defense-identical-twins/, Publicación sustraída fecha: 13/03/16

[239] Localizador de recursos uniforme (conocido por la sigla **URL**, del inglés *Uniform Resource Locator*) es un identificador de recursos uniforme (*Uniform Resource Identifier*, **URI**) cuyos recursos referidos pueden cambiar, esto es, la dirección puede apuntar a recursos variables en el tiempo. Están formados por una secuencia de caracteres, de acuerdo a un formato estándar, que designa recursos en una red, como Internet.

[240] Google Traductor – Del Inglés al Español.

apreciar de lo extraído por Trend Micro es un ataque mucho más elaborado para engañar a la víctima.

Trend Micro continúa describiendo este tipo de amenazas:

> *"Once the attacker has control of a machine on the inside of the corporate perimeter that can become a launching pad to probe for vulnerabilities on machines not directly connected to the internet. Often well-known techniques, for which patches have been available for some time, can succeed for the attacker in this situation because machines on the internal 'safe' network are not considered to be at risk by many companies. The human adversary directly controlling the compromised machine has the advantage of time ('Persistent') to quietly probe until they discover a weakness they can exploit."*[241]
>
> *"Una vez que el atacante tiene el control de una máquina en el interior del perímetro de la empresa que puede convertirla en una plataforma de lanzamiento para sondear en busca de vulnerabilidades en las máquinas que no están conectados directamente a Internet. A menudo las técnicas bien conocidas, para las que los parches han estado disponibles desde hace algún tiempo, pueden tener éxito para el atacante en esta situación porque las máquinas de la red interna "segura" no se consideran en riesgo por muchas empresas. El adversario humano que controla directamente el sistema afectado, tiene la ventaja de tiempo ('persistente') para sondear en silencio hasta que descubren una debilidad que pueden explotar."*[242]

Queda entonces, hasta el momento que el factor tiempo en este tipo de "ataques" es fundamental, esto claro con un trabajo bien elaborado con

---

241 TRENDMICRO.COM- Portal de Trend Micro**,** Cloud Security and APT defense – Identical Twins?
- http://blog.trendmicro.com/cloud-security-and-apt-defense-identical-twins/**,** Publicación sustraída fecha: 13/03/16

242 Google Traductor – Del Inglés al Español.

ingenieria social va a permitir que el atacante engañe a su víctima y logre conseguir tomar el control de la red interna.

- **Cloud Attacks – Ataques a la Nube**

Hoy en día las organización públicas y privadas entrelazan su información interna en lo que podríamos llamar un *SISTEMA CERRADO DIGITAL DE ALMACENAMIENTO EN INTERNET, QUE BRINDA LA POSIBILIDAD DE TRANSMITIR INFORMACION ENTRE PERSONAS RELACIONADAS A LA ACTIVIDAD DE LA EMPRESA PRIVADA O ENTIDAD PUBLICA*[243].

Dado que la *NUBE* ha revolucionado la forma de trasmitir información, y en muchos casos esta información tiene un valor en el mercado por el cual no puede difundirse, es por ello que los ciberataques en muchas casos van direccionados a nubes, debido a la gran cantidad de información que podemos almacenar, para ejemplificar podríamos tomar como ejemplo la Bóveda de un banco, son aparentemente seguras, se puede almacenar en ellas no solo dinero, sino también oro, documento de importancia; pero, las bóvedas a lo largo de la historia no han sido lo suficientemente seguras para evitar que las personas puedan violar su seguridad y acceder al contenido del interior, como ocurrió en *BRASIL*[244] en el año 2005, es por el desarrollo de las tecnologías en materia delictiva que se hace necesario reforzar la seguridad en todo sentido, porque la creatividad de los delincuentes se desarrolla constantemente creando nuevas y mejores formas de conseguir lo que buscan, de la misma forma y con mayor razón aun en el ***CIBERESPACIO NO HAY LÍMITES FÍSICOS QUE IMPIDAN QUE UN ATACANTE PUEDA ACCEDER A UNA "BÓVEDA" DIGITAL DE INFORMACIÓN, LO QUE NECESITA MUCHAS VECES ES INGENIO Y SABER UTILIZAR LAS HERRAMIENTAS NECESARIAS PARA PODER DIRECCIONAR SU ATAQUE***.

---

[243] Concepto del Tesista.

[244] "Entre el 6 y 7 de agosto del 2005, una banda de 35 ladrones irrumpió en las bóvedas del Banco Central de Fortaleza, en Brasil, a través de un túnel de 78 metros de largo que excavaron desde una casa vecina al edificio. El botín fue de US$86,4 millones. Al final todos fueron cayendo porque no se les ocurrió mejor idea que comprarse camionetas de lujo poco tiempo después del atraco". – "Estos son los 10 mayores robos de la historia", http/://elcomercio.pe/mundo/actualidad/estos-son-10-mayores-robos-historia-noticia-1749786, Publicado: 14/08/2014

Trend Micro a través de un artículo nos muestras como las nuevas propuesta pueden ayudar a mejor la realidad antes ataques realizados a los que se podría llegar a considerar una *"INFRAESTRUCTURA CRITICA DIGITAL DE SIGLO XXI"*, la versión mejorada de la *NUBE* ha sido desarrolla por *MICROSOFT*[245]*,* esta tecnología ofrecerá mejores estándares de seguridad, afirma que: *THAT 50% OF ENTERPRISES WOULD BE USING HYBRID CLOUDS BY 2017 – QUE EL 50% DE LAS EMPRESAS ESTARIAN UTILIZANDO LA NUBE HIBRIDA PARA EL 2017*[246]*.*

Acerca de la *NUBE HIBRIDA*, *TREND MICRO* la describe de la siguiente forma:

> *"The hybrid cloud is a key component of the Software-Defined Data Center, where the entire infrastructure of the data center is managed and controlled through intelligence software systems as opposed to hardware. It means compute, storage and networking capabilities can be provisioned in seconds rather than days or weeks. But it also requires software-defined security to fully leverage these advantages."*[247]
>
> *"La nube híbrida es un componente clave del CENTRO DE DEFINICION DE DATOS POR SOFTWARE, donde se gestiona toda la infraestructura del CENTRO DE DATOS y es controlado a través de sistemas de software de inteligencia en lugar de hardware. Significa cómputo, almacenamiento y capacidades de red puede aprovisionarse en cuestión de segundos en lugar de días o semanas. Pero también requiere de seguridad definida por software para aprovechar plenamente estas ventajas."*[248]

---

[245] Empresa multinacional de origen estadounidense, fundada el 4 de abril de 1975 por Bill Gates y Paul Allen. Dedicada al sector del software y el hardware.

[246] Google Traductor – Del Inglés al Español.

[247] TRENDMICRO.COM- Portal de Trend Micro**,** Hybrid Cloud: Going Beyond Security in a Software Defined Datacenter **-**http://blog.trendmicro.com/hybrid-cloud-going-beyond-security-software-defined-datacenter/**, Publicación sustraída fecha: 16/03/16**

[248] Google Traductor – Del Inglés al Español.

MICROSOFT apuesta entonces por la tecnología del software derivando toda la tarea de almacenamiento y de seguridad a softwares que reemplazarían a los servidores o computadores, esto evidentemente por la diferencia con respecto a capacidades que muestran cada una de las tecnologías.

El siguiente punto que tocaremos, no podría ser considerado como un ciberataque pero su creación tiene como resultado que actividades ilicitas como el comercio ilegal de armas, el tráfico ilícito de drogas, la comercialización de actividades como el sicariato o la trata de personas, se desarrollen, es la llamada *DEEP WEB – LA RED PROFUNDA y LA DARK WEB – RED OSCURA*[249], para ejemplificar esto utilizaremos la siguiente imagen:

249 https://www.google.com.pe/search?q=la+deep+web+imagen&espv=2&biw=1280&bih=923&tbm=isch&imgil=QmnwOWj_wJQbOM%253A%253B5-eH9Yrp_ZsWYM%253Bhttps%25253A%25252F%25252Fpulsionesblog.wordpress.com%25252F2013%25252F12%25252F17%25252Fcronica-navegando-por-la-deep-web%25252F&source=iu&pf=m&fir=QmnwOWj_wJQbOM%253A%252C5-eH9Yrp_ZsWYM%252C_&usg=__Ufmp0r360nOwMlHyMbqioNv7Kq0%3D&ved=0ahUKEwjX37_BwbfNAhWMKCYKHfhIDNoQyjcINQ&ei=G1toV5fmHIzRmAH4kbHQDQ#imgrc=QmnwOWj_wJQbOM%3A, extraido el 14/04/2016

Es así que podemos entender que el ciberespacio tiene varios niveles, la mayoría de usuarios de la web utilizamos solo el 10% de toda la web.

- **Deep Web – Red Profunda**

Desarrollar el presente punto nos pone en una situación en la que se hace necesario conocer todo lo que implica la internet, y dejar en claro concepto básicos para así poder entrar en el conceptualizar a la famosa *DEEP WEB*.

La *OTAN,* en ese sentido a desarrollado un trabajo básico, que todo especialista debería tener en claro para desenvolverse en temas ciber. Así la *OTAN* sobre la internet nos dice:

> *"The internet is a network of networks, linking computers to computers sharing the TCP/IP protocols. Each runs software to provide or "serve" information and/or to access and view information."*[250]
>
> *"El Internet es una red de redes, la vinculación los ordenadores a ordenadores que comparten los protocolos TCP / IP*[251]*. Cada uno ejecuta el software para proporcionar o "servir" a la información y / o para acceder y ver la información."*[252]

Una pregunta en este punto seria: *ENTONCES LA INTERNET ES INFORMACION?* Pues no, *LA INTERNET ES UNA RED QUE FACILITA EL INTERCAMBIO DE INFORMACIÓN Y LA COMUNICACION A NIVEL MUNDIAL, LA INTERNET POR SÍ SOLA NO BRINDA INFORMACIÓN, SON LOS USUARIOS QUE A TRAVÉS DE SUS ORDENADORES QUE ALIMENTAN A LA INTERNET DE*

---

[250] NATO.INT – Portal de la OTAN, INTELLIGENCE EXPLOITATION OF THE INTERNET - http://nsarchive.gwu.edu/NSAEBB/NSAEBB436/docs/EBB-005.pdf, Información sustraída: 24/03/2016

[251] *Transmission Control Protocol/Internet Protocol - protocolo de control de transmisión/protocolo de Internet*. Protocolos de Internet que cada usuario Internet y cada servidor de Internet usa para comunicar y transferir datos sobre las redes. El TCP empaqueta datos en los paquetes que se envían en Internet y se vuelven a montar en sus destinos. El IP maneja la dirección y el enrutamiento de cada paquete de datos de forma que se envía al destino correcto. – SYMANTEC.COM, Portal de Symantec http://www.symantec.com/es/mx/security_response/glossary/define.jsp?letter=t&word=tcp-ip-transmission-control-protocol-internet-protocol, Información sustraída: 24/03/2016

[252] Google Traductor – Del Inglés al Español.

INFORMACIÓN, A TRAVÉS DE TODO UN SISTEMA INTERCONECTADO DE SERVIDORES QUE FACILITAN EL COMPARTIR LA INFORMACIÓN ENTRE LOS USUARIOS.[253]

La *OTAN* continúa ilustrándonos de la siguiente manera:

> *"The internet is the transport vehicle for the information stored in files or documents on another computer. It can be compared to an international communications utility servicing computers."*[254]
>
> *"La Internet es el vehículo de transporte de la información almacenada en los archivos o documentos en otro equipo. Se puede comparar con una herramienta de comunicación internacional mantenida por computadoras."*[255]

La internet según la *OTAN* es el vehículo que facilita, siendo necesario para esto que se le alimente de información, es ahí donde los usuarios tomamos un papel preponderante en la labor de suministrar a esta red información, basándonos siempre en el hecho de que *ALGUIEN PUEDE ESTAR INTERESADO EN LO QUE NOSOTROS DECIMOS O HACEMOS.*

La internet y la deep web están relacionadas? Pues si, la deep web es una parte del internet, y como tal, facilita el intercambio de información. Según la *OTAN:*

> *"The invisible web is composed of web pages that can be accesed via the internet, but are not found by searchs engines. These are pages that are either located too "deep" in a web site for a search engine´ s spider to located, are pages that a search engine cannot index because it technically cannot do so, or are pages which*

[253] Concepto del Tesis.
[254] NATO.INT – Portal de la OTAN, INTELLIGENCE EXPLOITATION OF THE INTERNET - http://nsarchive.gwu.edu/NSAEBB/NSAEBB436/docs/EBB-005.pdf, pp. 7, Información sustraída: 24/03/2016
[255] Google Traductor – Del Inglés al Español.

the search engine cannot access because they lack the proper password."[256]

"La red invisible se compone de páginas web que se puede acceder a través de Internet, pero no se encuentran por los motores de búsqueda. Estas son páginas que están ubicados demasiado "profundo" en un sitio web, en donde un motor de búsqueda no puede localizar, son páginas que un motor de búsqueda no pueden indexar, ya que técnicamente no puede hacerlo, o son páginas de las que el motor de búsqueda no puede acceder porque carece de la contraseña correcta."[257]

Es necesario aclarar que la deep web es conocida por la *OTAN* como la red invisible, a la que según nos dice, es difícil acceder bien sea por las contraseñas o por que se encuentran indexadas de manera distinta y haga imposible que el *MOTOR DE BÚSQUEDA*[258] puede acceder a ellas.

Entonces, *PARA QUE ES UTILIZADA LA DEEP WEB?* Según Trend Micro, la deep web es utilizada:

"A smart person buying recreational drugs online wouldn't want to type related keywords into a regular browser.
He/She will need to anonymously go online using an infrastructure that will never lead interested parties to his/her IP address or physical location. Drug sellers wouldn't want to set up shop in an online location whose registrant law enforcement can easily determine or where the site's IP address exist in the real world, too."

---

[256] NATO.INT – Portal de la OTAN, INTELLIGENCE EXPLOITATION OF THE INTERNET - http://nsarchive.gwu.edu/NSAEBB/NSAEBB436/docs/EBB-005.pdf, pp. 51 Información sustraída: 24/03/2016

[257] Google Traductor – Del Inglés al Español.

[258] Un motor de búsqueda, también conocido como buscador, es un sistema informático que busca archivo almacenados en servidores web gracias a su «*spider*» (también llamado araña web). Un ejemplo son los buscadores de Internet (algunos buscan únicamente en la web, pero otros lo hacen además en noticias, etc.) cuando se pide información sobre algún tema. Las búsquedas se hacen con palabras clave o con árboles jerárquicos por temas; el resultado de la búsqueda «Página de resultados del buscador» es un listado de direcciones web en los que se mencionan temas relacionados con las palabras clave buscadas. - https://es.wikipedia.org/wiki/Motor_de_b%C3%BAsqueda, Información sustraída: 24/03/2016

"Una persona inteligente para comprar drogas recreativas en línea no querría escribir palabras clave relacionadas en un habitual navegador.

El / ella tendrá que ir de forma anónima en línea utilizando una infraestructura que nunca producirá interés en su dirección IP o la ubicación física. Los traficantes de drogas no quieren instalarse en donde las leyes puedan determinar con facilidad su ubicación o la ubicación en el mundo real de la dirección IP."[259]

La deep web entonces es un mercado "seguro" para comercializar drogas*?* o solo es utilizada para este fin? Pues no, Trend Micro nos dice:

"There are many other reasons, apart from buying drugs, why people would want to remain anonymous or set up sites that can't be traced back to a physical location or entity. People who want to shield their communications from government surveillance may require the cover of darknets. Whistleblowers may want to share vast amounts of insider information to journalists without leaving a paper trail. Dissidents in restrictive regimes may need anonymity in order to safely let the world know what's happening in their country.

On the flip side, people who want to plot the assassination of a high-profile target will want a guaranteed but untraceable means. Other illegal services like selling documents such as passports and credit cards also require an infrastructure that guarantees anonymity. The same can be said for people who leak other people's personal information like addresses and contact details."[260]

[259] TRENDMICRO.COM-Portal de Trend Micro, BELOW THE SURFACE: EXPLORING THE DEEP WEB - https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_below_the_surface.pdf, pp. 6, Información sustraída: 24/03/2016

[260] Loc. Cit. idem. - https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_below_the_surface.pdf, Información sustraída: 24/03/2016

"Hay muchas otras razones, además de la compra de drogas, por las qué la gente quiere permanecer en el anonimato o crear sitios web que no se pueden rastrear a una ubicación física o entidad. Las personas que quieren proteger sus comunicaciones de vigilancia del gobierno pueden requerir la protección de la "oscuridad". Los denunciantes pueden querer compartir grandes cantidades de información privilegiada a los periodistas sin dejar un rastro de papel. Dirigentes en regímenes restrictivos pueden necesitar el anonimato con el fin de dejar con seguridad que el mundo sepa lo que está sucediendo en su país.

Por otro lado, las personas que quieren trazar el asesinato de un blanco de alto perfil querrán garantizar que los medios no puedan rastrearlos. Otros servicios ilegales como la venta de documentos como pasaportes y tarjetas de crédito también requieren una infraestructura que garantiza el anonimato. Lo mismo puede decirse de las personas que se escapan de otras personas como su información personal, direcciones y datos de contacto."[261]

Hasta el momento relacionar a la deep web con lo *ilegal* es inevitable, pero es siempre así? La deep web tiene solo fines ilícitos? Pues no, Trend Micro nos dice:

"While there are, of course, sites dedicated to drugs and weapons, a huge chunk of Deep Web sites are dedicated to more mundane topics—personal or political blogs, news sites, discussion forums, religious sites, and even radio stations. Just like sites found on the Surface Web, these niche Deep Web sites cater to individuals hoping to talk to like-minded people, albeit anonymously."[262]

[261] Google Traductor – Del Inglés al Español.
[262] TRENDMICRO.COM-Portal de Trend Micro, BELOW THE SURFACE: EXPLORING THE DEEP WEB - https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_below_the_surface.pdf, pp. 8, Información sustraída: 24/03/2016

> *"…Si bien hay, por supuesto, los sitios dedicados a las drogas y las armas, una gran parte de los sitios en la web profunda se dedican a los blogs de los temas más mundanos-personales o políticos, sitios de noticias, foros de discusión, sitios religiosos, e incluso las estaciones de radio. Al igual que los sitios que se encuentran en la web de la superficie, estos sitios Web de la Web profunda atienden a personas con la esperanza de hablar con personas de ideas afines, aunque sea de forma anónima."*[263]

La deep web es entonces *UN ESPACIO DENTRO DE LA INTERNET EN LA CUAL LOS USUARIOS PUEDEN DESARROLLAR ACTIVIDADES DIVERSAS CON UN ALTO GRADO DE "ANONIMATO" RESPECTO A SU UBICACIÓN O IDENTIDAD.*[264]

- **Dark Web – Red Oscura**

Actualmente no existe mucha información con respecto a la *DARK WEB*, se sabe que es una parte de la deep web pero no son lo mismo una y otra. Con respecto a la dark web, Trend Micro nos da el siguiente alcance:

> *"The Dark Web relies on darknets or networks where connections are made between trusted peers."*[265]

> *"El Dark Web se basa en darknets*[266] *o redes donde las conexiones se realizan entre pares de confianza."*[267]

---

[263] Google Traductor – Del Inglés al Español.
[264] Concepto del Tesista.
[265] TRENDMICRO.COM-Portal de Trend Micro, BELOW THE SURFACE: EXPLORING THE DEEP WEB - https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_below_the_surface.pdf, pp. 6, Información sustraída: 24/03/2016
[266] *Darknets refer to a class of networks that aim to guarantee anonymous and untraceable access to Web content and anonymity for a site. - Darknets se refieren a una clase de redes que tienen como objetivo garantizar el acceso anónimo e indetectable para el contenido web y el anonimato de un sitio*. – TREND MICRO.COM – Portal de Trend Micro, Deep Web and Cybercrime: It's Not All About Tor - http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/deep-web-and-cybercrime-its-not-all-about-tor, Información sustraída: 25/03/2016
[267] Google Traductor – Del Inglés al Español.

La dark web, es la parte más profunda de la deep web, en este punto presumir que todas las actividades que se desarrollan en ella son delictivas seria asumir una presunción carente de pruebas, como hemos visto en la deep web no solo se desarrollan actividades delictivas sino otro tipo de actividades que no afectan a la ciberseguridad.

Como la dark web y la deep web son distintas, *ES POSIBLE ACCEDER A CUALQUIERA DE LAS DOS A TRAVÉS LOS MISMOS MEDIOS? O CON LOS MISMO CONOCIMIENTOS TECNICOS*? Preguntarnos esto es necesario, porque si bien nos ha quedado claro que no es lo mismo, establecer más diferencias entre una y otra ayudaría más a delimitar un concepto acerca de ambas. Para ello Trend Micro nos dice:

> *"…The Dark Web would be the deeper portions of the Deep Web that require highly specialized tools or equipment to access. It lies deeper underground and site owners have more reason to keep their content hidden."*[268]

> *"…El Dark Web sería la parte más profunda de la Web profunda que requiere herramientas o equipos altamente especializados para el acceso. Está a mayor profundidad y los propietarios del sitio tienen más razón para mantener su contenido oculto"*[269]

En definitiva se puede presumir que actividades ilícitas se pueden llevar acabo en un ambiente como estos, por ejemplo podemos utilizar a manera de ejemplo al *SILKROAD,* para ello seguiremos utilizando a Trend Micro como referente:

> *"The SilkRoad was the most notorious example of an online marketplace found in the Tor network. Before it was taken down by the FBI in 2013, the website was used*

[268] TRENDMICRO.COM-Portal de Trend Micro, BELOW THE SURFACE: EXPLORING THE DEEP WEB - https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_below_the_surface.pdf, pp. 6, Información sustraída: 24/03/2016
[269] Google Traductor – Del Inglés al Español.

as a platform for selling illegal drugs, where users were able to browse anonymously."[270]

"La SilkRoad (Ruta de Seda) fue el ejemplo más notorio de un mercado en línea que se encontraba en la red Tor. Antes de que fuera bajado por el FBI en 2013, el sitio fue utilizado como una plataforma para la venta de drogas ilegales, donde los usuarios fueron capaces de navegar de forma anónima."[271]

Con lo dicho es posible sentir una brisa de seguridad contra lo que ocurre en la internet debido a que organización como el *FBI* son capaces de tomar acciones contra este tipo de sitios web en donde la comercialización de sustancias ilícitas es el "objeto social" de este *CIBERPERSONAJE* llamado silkroad.

Pero esa brisa de seguridad que sentimos cuando el *FBI* logro desarticular este gran mercado, sucede lo siguiente:

"That wasn't the end of it though, as a new site soon took its place on November 6th, 2013. Called "Silk Road 2.0", the relaunched site promised improved security to avoid another shutdown. On November 6, 2014, exactly one year after the launch of Silk Road 2.0, the new site was shut down and its operator was arrested through the efforts of Operation Onymous—an international law enforcement operation that targets illegal online marketplaces operating in the Tor network." [272]

"Ese no fue el final de la misma, abrió como un nuevo sitio de pronto tomó su lugar el 6 de noviembre de 2013.

---

270 TREND MICRO.COM – Portal de Trend Micro, Deep Web and Cybercrime: It's Not All About Tor - http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/deep-web-and-cybercrime-its-not-all-about-tor, Información sustraída: 25/03/2016

271 Google traductor – Del Inglés al Español.

272 TREND MICRO.COM – Portal de Trend Micro, Deep Web and Cybercrime: It's Not All About Tor - http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/deep-web-and-cybercrime-its-not-all-about-tor, Información sustraída: 25/03/2016

Se llama "ruta de la seda 2.0", el sitio relanzado prometió una mayor seguridad para evitar otro cierre. El 6 de noviembre de 2014, exactamente un año después del lanzamiento de la Ruta de la Seda 2.0, el nuevo sitio fue cerrado y su operador fue detenido por los esfuerzos de la Operación Onymous-una operación policial internacional que se dirige a mercados ilegales en línea que operan en la red Tor."[273]

No podemos cerrar la sección sin antes establecer la clara diferencia entre lo que es la Ciberseguridad y la Ciberdefensa, si bien ambos termino han sido utilizado en la presente investigación, se hace necesario determinar que son, establecer en que momento debemos hablar de una y otra.

- **Ciberseguridad Experiencia Internacional**

Comenzaremos vertiendo diversos conceptos, como el siguiente:

"Measures relating to the confidentially, availability and integrity of information that is processed, stored and communicated by electronic or similar means."[274]

"Las medidas relativas a la confidencialidad, disponibilidad e integridad de la información que se procesa, almacena y comunicada por medios electrónicos o similares."[275]

El presente concepto es el utilizado por Australia, para la realidad Australiana, la Ciberseguridad son las medidas que se utilizan para proteger la información, entonces estamos hablando de que la Ciberseguridad no solo es la creacion de un ordenamiento jurídico acorde a la realidad si no también se necesita de otro tipo de herramientas, es por ellos que la palabra "medidas" es precisa por la amplitud de mecanismos que podemos utilizar para la correcta implementación de la Ciberseguridad.

"Cyber security describes the protection of a key legal asset through constitutional means against actor-related,

[273] Google Traductor – Del Inglés al Español.
[274] NATO.INT – Portal de la OTAN, Centro de Excelencia de la OTAN- https://ccdcoe.org/cyber-definitions.html, Información sustraída: 22/05/2016
[275] Google Traductor – Del Ingles al Español

technical, organisational and natural dangers posing a risk to the security of cyber space (including infrastructure and data security) as well as the security of the users in cyber space. Cyber security helps to identify, assess and follow up on threats as well as to strengthen the ability to cope with interferences in or from cyber space, to minimise the effects as well as to restore the capacity to act and functional capabilities of the respective stakeholders, infrastructures and services."[276]

"La seguridad cibernética describe la protección de un bien jurídico fundamental a través de medios constitucionales contra el actor relacionado, peligros técnicos, organizativos y naturales que suponen un riesgo para la seguridad del espacio cibernético (incluyendo la infraestructura y la seguridad de los datos), así como la seguridad de los usuarios en la lucha del espacio virtual. La seguridad informática ayuda a identificar, evaluar y dar seguimiento a las amenazas, así como para fortalecer la capacidad de hacer frente a las interferencias en o desde el espacio cibernético, para minimizar los efectos, así como para restaurar la capacidad de actuar y las capacidades funcionales de los respectivos grupos de interés, infraestructuras y servicios."[277]

El concepto proviene de Austria, lo reconocen como un bien jurídico que debe ser defendido a traves de medio constitucionales, con lo cual se entiende que el ordenamiento jurídico debe de adecuarse no solo a nivel constitucional si con normas de inferior jerarquía que sirvan para que el Estado accione en determinadas situaciones, minimizando los efectos.

"The desired state of an information system in which it can resist events from cyberspace likely to compromise the

[276] NATO.INT – Portal de la OTAN, Centro de Excelencia de la OTAN- https://ccdcoe.org/cyber-definitions.html, Información sustraída: 22/05/2016
[277] Google Traductor – del Ingles al Español

availability, integrity or confidentiality of the data stored, processed or transmitted and of the related services that these systems offer or make accessible. Cybersecurity makes use of information systems security techniques and is based on fighting cybercrime and establishing cyber defence."[278]

"El estado deseado de un sistema de información en el que se puede resistir eventos desde el ciberespacio que podrían poner en peligro la disponibilidad, integridad y confidencialidad de los datos almacenados, procesados o transmitidos y de los servicios relacionados que estos sistemas ofrecen o hacen accesibles. Ciberseguridad hace uso de las técnicas de seguridad de sistemas de información y se basa en la lucha contra la delincuencia informática y el establecimiento de defensa cibernética."[279]

Francia nos da un alcance mayor haciendo referencia a las tecnicas de seguridad de sistemas de informacion, con lo cual que clara que la disciplina de Ciberseguridad es una disciplina la cual debe ser abordada de manera multisectorial, como vemos en las 3 experiencias de países como Australia, Austria y Francias, nos solo es necesario la adecuación jurídica sino es necesaria la implementación técnica en la materia.

- **Ciberdefensa**

Habiendo ya aclarado lo que es la Ciberseguridad nos toca establecer lo que es la Ciberdefensa para ellos utilizaremo la misma metodología utilizada para la Ciberseguridad.

[278] NATO.INT – Portal de la OTAN, Centro de Excelencia de la OTAN- https://ccdcoe.org/cyber-definitions.html, Información sustraída: 22/05/2016
[279] Google Traductor – Del Ingles al Español.

"organized capabilities to protect against, mitigate from and rapifly reciver frim the effects of cyber attack"[280]
"capacidades organizadas para proteger contra, mitigar y recuperación rápida de los efectos de ataques cibernéticos"[281]

Como podemos, la experiencia Rusa define a la Ciberdefensa como la capacidad de reacción frente a incidente ciberneticos.

"The set of all technical and non-technical measures allowing a State to defend in cyberspace information systems that it considers to be critical."[282]

"El conjunto de todas las medidas técnicas y no técnicas que permiten a un Estado defenderse en los sistemas de información del ciberespacio que consideran ser crítico."[283]

Francia lo reconoce como las medidas frente a un incidente cibernetico, ahora bien lo interesante de la concepción francesa es lo referente a "Tecnico y no Tecnico" para ejercer la defensa del Estado, es un alcance que en definitiva ayuda a entender que en una situación de conflicto el Estado esta en la necesidad de defenderse.

"The application of effective protective measures to obtain an appropriate level of Cyber Security in order to guarantee Defence`s operation and functionalities. This is achieved by applying appropriate protective measures to reduce the security risk to an acceptable level. Cyber Defence consists

[280] NATO.INT – Portal de la OTAN, Centro de Excelencia de la OTAN- https://ccdcoe.org/cyber-definitions.html, Información sustraída: 22/05/2016
[281] Google Traductor – Del Ingles al Español.
[282] NATO.INT – Portal de la OTAN, Centro de Excelencia de la OTAN- https://ccdcoe.org/cyber-definitions.html, Información sustraída: 22/05/2016
[283] Google Traductor – Del Ingles al Español.

of following duties: Protect, Detect, Respond, and Recover"[284]

"La aplicación de medidas de protección efectivas para obtener un nivel apropiado de Seguridad Cibernética con el fin de garantizar el funcionamiento y las funcionalidades de la Defensa. Esto se logra mediante la aplicación de medidas de protección adecuadas para reducir el riesgo de seguridad a un nivel aceptable. Ciberdefensa consiste siguientes funciones: proteger, detectar, responder y recuperar"[285]

Desde nuestro punto de vista el concepto brindado por Belgica, es el concepto que mas nos ayuda a aterrizar lo que Ciberdefensa es, es necesario entender que con buenas medidas de Ciberseguridad se lograra elevar lo niveles de Ciberdefensa con lo cual el Estado se encontrara en una mejor situación frente a un incidente cibernetico.

Otro punto que es necesario establecer es que ***la Ciberdefensa tiene como función protegeré, detectar, responder y recuperar mientras que la Ciberseguridad serán las medidas para garantizar que los sistemas informaticos y ciberneticos se encuentra protegidos, esto a traves de todo un adamiaje de herramientas que van desde el ordenamiento jurídico hasta las herramientas tecnicas.***

No es necesario ser un gran analista en materia de *CIBERSEGURIDAD*, con tan solo conocer un poco sobre la realidad nacional, el Perú en definitiva no se encuentra preparado para poder detectar o desarticular, si alguna organización decide introducirse en el mercado de sustancias prohibidas y comercializarlas en la *DEEP WEB* o la *DARK WEB,* el Perú no cuenta con los medios necesarios para poder realizar acciones contra una organización delictiva, esto por varias razones. En este punto no pretendemos profundizar

[284] NATO.INT – Portal de la OTAN, Centro de Excelencia de la OTAN- https://ccdcoe.org/cyber-definitions.html, Información sustraída: 22/05/2016
[285] Google Traductor – Del Ingles al Español.

sobre el tema, solo lo mencionamos a manera de introducción para su posterior desarrollo.

CUARTO CAPITULO

1. Realidad Nacional – Políticas de CiberSeguridad – Legislación en Ciberseguridad y Ciber Defensa.

En el presente capitulo analizaremos la realidad Peruana, de forma multidisciplinaria, comenzaremos vertiendo una de las enseñanzas del *GENERAL CHINO SUN TZU*, y lo que considera sobre el primer aspecto que tocaremos:

> *"**El terreno** implica las distancias, y hace referencia a dónde es fácil o difícil desplazarse, y si es campo abierto o lugares estrechos, y esto influencia las posibilidades de supervivencia."*[286]

Consideramos necesario precisar lo siguiente, la ciberseguridad y la ciberdefensa*,* son dos conceptos distintos pero relacionados íntimamente uno con otro, buenas políticas de ciberseguridad conllevaran a una buena posición en ciberdefensa. Así mismo consideramos necesarios hacer otra precisión, la ciberseguridad es un concepto que se va a aplicar a través de una relación de subordinación entre el Estado como garante principal de la seguridad y los habitantes de su territorio, mientras que la ciberdefensa se debe entender como la posición del Estado frente a ataques que afectan a la soberania del Estado, que a diferencia de las guerra convencionales, estas no siempre son accionadas por otro Estado sino, como ya hemos visto, líneas arriba, el ataque podría venir de cualquier parte del mundo y podría ser una *ORGANIZACIÓN CIBERTERRORISTA.*

Es necesario entonces realizar el análisis respectivo del aspecto físico de la realidad Peruana, si bien la característica de "*TERRITORIALIDAD"* no es un determinante para una disciplina como la ciberdefensa o ciberseguridad*,* esto debido a que la internet hace posible el ataque provenga de cualquier parte del mundo, ahora bien, si la territorialidad no es característica principal de ambas disciplinas tampoco podríamos decir no es necesario establecer

[286] SUN TZU, El Arte de la Guerra, Capítulo I pp.3

territorialmente políticas, normas, estrategias, directivas, protocolos que ayuden a mejorar la seguridad cibernetica[287].

Pero ¿POR QUE DECIR QUE EN LA CIBERSEGURIDAD Y LA CIBERDEFENSA NO ES UNA CARACTERISTICA PRINCIPAL LA TERRITORIALIDAD? ¿ACASO NO AFECTA LA SOBERANIA DE LOS ESTADO? Para responder a la primera pregunta la realidad creada por internet rompe cualquier limite físico, al afirmar esto es necesario precisar que como la mayoría de actividades humanas, esta también se le puede dar un uso beneficioso como uno maligno, entonces mientras algunas persona utilizan la internet para romper los limites físico y mantener un conversación con personas que se encuentran una en polo norte y el otro en el polo sur, habrán personas por otro lado que lo que buscaran en la internet es romper límites físicos para cometer ciberdelitos, por ejemplo una persona con conocimientos técnicos lanza un ataque desde Alaska a un servidor en China para afectar usuarios en América del Sur. Para responder a la segunda pregunta: Pues si, en definitiva afecta a la soberania de los Estados, claro debido a la magnitud del ataque afectara en mayor o menor medida y dependiendo de a que este direccionado el ataque.

En este punto viene la pregunta que justificara la primera parte de este capítulo ¿ENTONCES QUE NORMA SERA LA QUE SE LE APLICARA AL CIBERCRIMINAL? Seria gracias a esta última pregunta que nosotros podremos desarrollar la territorialidad como elemento de la ciberdefensa y ciberseguridad.

Consideramos necesario analizar porque el elemento territorialidad no puede eliminarse de los elementos que conforman la ciberdefensa y ciberseguridad, por un lado encontraremos que eventualmente será necesario aplicarle una sanción, sea esta penal o administrativa, a un cibercriminal, y esto será posible, una vez que entendamos que es necesario impulsar el desarrollo de las tecnologías para proteger nuestros sistemas informáticos y ciberneticos, en todo caso será necesario poder aplicarle una sanción al cibercriminal,

[287] Cibernética.- Ciencia que estudia las analogías entre los sistemas de control y comunicación de los seres vivos y los de las maquinas.

utilicemos el ejemplo anterior: *UNA PERSONA CON CONOCIMIENTOS TÉCNICOS LANZA UN ATAQUE DESDE ALASKA A UN SERVIDOR EN CHINA PARA AFECTAR USUARIOS EN AMÉRICA DEL SUR,* el sujeto pasivo de la acción se encuentra en diferentes países de América del Sur pero cuál será el ordenamiento que deba aplicar la sanción?

Con respecto a la cuestión relacionada a que Estado tendría la jurisdicción para juzgar a un ciberdelincuente en caso que el sujeto activo no se encuentre en el país en donde el sujeto pasivo de encuentra, la OTAN establece algunos criterios para determinar la jurisdicción.

Como ya hemos establecido la Soberanía no va a hecho de regular el Ciber Espacio, si no regula la actividad de las infraestructuras cibernéticas que se encuentran dentro de su territorio, al cual se puede aplicar a través de su poder soberano su jurisdicción. Para esto la OTAN nos dice:

> *"Without prejudice to applicable international obligations, a State may exercise it´s jurisdiction:*
> *a) over persons engaged in cyber activities on its territory;*
> *b) over cyber infrastructure located on its territory; and*
> *c) extraterritorially, in accordance with international law."*[288]

> *"Sin perjuicio de las obligaciones internacionales aplicables, un Estado puede ejercer su jurisdicción:*
> *a) respecto de las personas que participan en actividades cibernéticos en su territorio;*
> *b) sobre la infraestructura cibernética situada en su territorio; y*
> *c) fuera del territorio, de conformidad con el derecho internacional."*[289]

[288] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE. Cambridge University Press, pp. 18.
[289] Google traductor – Del Inglés al Español.

Para desarrollar la idea anterior, la OTAN continua de la siguiente forma:

> *"The principal basis for a State to exercise its jurisdiction is physical o legal presence of a person (in personam) or object (in rem) on its territory. For instance, pursuant to its in personam jurisdiction a State may adopt laws and regulations governing the cyber activities of individuals on its territory. It may also regulate the activities of privately owned entities registered (or otherwise based as a matter of law) in its jurisdiction but physically operating abroad, such as Internet service providers (ISP´s). In rem jurisdiction would allow it to adopt laws governing the operation of cyber infrastructure on its territory."*[290]
>
> *"La base principal para un Estado ejerza su jurisdicción es física o la presencia legal de una persona (in personam) u objeto (in rem) en su territorio. Por ejemplo, en virtud de su jurisdicción in personam un Estado puede adoptar leyes y reglamentos que regulan las actividades cibernéticas de las personas en su territorio. También puede regular la actividad de las entidades de propiedad privada registradas (o de otro tipo basados como una cuestión de derecho) en su jurisdicción, pero que operan físicamente en el extranjero, como los proveedores de servicios de Internet (ISP's). Jurisdicción in rem permitiría a adoptar leyes que rigen el funcionamiento de la infraestructura cibernética en su territorio."*[291]

Entonces con respecto a la jurisdicción de un Estado en el ámbito Ciber, se encuentra relacionado a las personas que estas pueden personas naturales o personas jurídicas, también puede ejercer su jurisdicción a personas jurídicas que se encuentra registradas en su territorio pero que operan físicamente fuera del territorio.

[290] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE. Cambridge University Press, pp. 18.
[291] Google traductor – Del Inglés al Español.

La principal complejidad que encuentra el aplicar la jurisdicción de un Estado y otro, es que en Internet, se puede estar en diferentes jurisdicciones al mismo tiempo, así como estar en ninguna jurisdicción.

> *"It be difficult to determine jurisdiction within cyberspace because cloud or grid distributed systems can span national borders, as can the replication and dynamic relocation of data and processing. This makes it challenging at any particular time to determine where all of a user´s data and processing reside since such data can be located in multiple jurisdiction simultaneously. These technical challenges do not deprives a State of its legal rights to exercise jurisdiction over persons and cyber infrastructure located on its territory."* [292]

> *"Es difícil determinar la jurisdicción dentro del ciberespacio, porque los sistemas de nubes o de cuadrícula distribuida pueden atravesar fronteras nacionales, al igual que la replicación y la reubicación dinámica de los datos y su procesamiento. Esto hace que sea difícil en cualquier momento particular determinar donde todo el conjunto de datos y el procesamiento de usuarios residen ya que dichos datos pueden ser localizados en múltiples jurisdicciones simultáneamente. Estos desafíos técnicos no priva a un Estado de sus derechos legales para ejercer su jurisdicción sobre personas y la infraestructura cibernética ubicados en su territorio."*[293]

Queda claro que la jurisdicción con respecto a personas y a entidades sean públicas o privadas se ejercerá a través del Estado en el que se encuentran o hayan sido registradas, pero que ocurre si se utilizar dispositivos móviles? Qué ocurre si el dispositivo móvil se desplaza a otro país?

[292] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE. Cambridge University Press, pp. 19.
[293] Google traductor – Del Inglés al Español.

"With regard to jurisdiction based upon territoriality, it must be noted that although individuals using information and communications technology have a specific physical location, the location of mobile devices can change during a computing session. For instance, a person with a mobile computing device (e.g. a tablet or smartphone) can initiate several database queries or updates for processing by cloud-based service. As those queries and updates take place, the user may move to another location. Any State from which the individual has operated enjoys jurisdiction because the individual, and the device involved, were located on its territory when so used."[294]

"Con respecto a la jurisdicción basada en la territorialidad, hay que señalar que si bien las personas que utilizan la tecnología de la información y las comunicaciones tienen una ubicación física específica, la ubicación de los dispositivos móviles puede cambiar durante una sesión de la computación. Por ejemplo, una persona con un dispositivo de computación móvil (por ejemplo una tablet o teléfono inteligente) puede iniciar varias consultas de bases de datos o actualizaciones para el procesamiento a través del servicio basado en la nube. Como esas consultas y actualizaciones se llevan a cabo, el usuario puede desplazarse a otro lugar. Cualquier Estado desde el que ha operado el individuo goza de jurisdicción porque el individuo, y el dispositivo implicado, se encuentran en su territorio cuando se utiliza."[295]

Los dispositivos móviles fue un desafío para el establecimiento de la jurisdicción, fue ahí donde la tecnología aporto un elemento para que los

[294] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE. Cambridge University Press, pp. 19.
[295] Google traductor – Del Inglés al Español.

Estados tomen en cuenta al momento de establecer la jurisdicción que aplicaría.

> *"Even with technology such as mobile cloud computing, the devices from which the human user is initiating requests can be goe-located; software services and applications may track the geo-coordinates of the computing device (e.g. Wifi connection location or the devices global positioning system (GPS) location). It must be cautioned that it is possible under certain circumstances for someone who does not wish to be tracked to spoof the geo-coordinates advertised by his or her computing device. It is also possible the user-location will not be made available by the infrastructure or service provider, or by the application or device itself. Actual physical presence is required, and sufficient, for jurisdiction based on territoriality; spoofed presence does not suffice."*[296]

> *"Incluso con la tecnología móvil como la computación en nube, los dispositivos desde los cuales el usuario humano está iniciando peticiones pueden ser geo-ubicados; servicios de software y aplicaciones pueden realizar un seguimiento de las coordenadas geográficas del dispositivo informático (por ejemplo, ubicación de la conexión Wi-Fi o el sistema de posicionamiento global (GPS) de ubicación). Debe advertirse que es posible bajo ciertas circunstancias para alguien que no quiere ser rastreados que simule las coordenadas geográficas anunciadas por su dispositivo de computación. También es posible que la ubicación del usuario no esté disponible por el proveedor de infraestructura o servicio, o por la aplicación o dispositivo en sí. Se requiere la presencia física, y suficiente, para la*

[296]TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE. Cambridge University Press, pp. 19.

jurisdicción basada en la territorialidad; presencia falsificada no es suficiente."[297]

Ahora bien, para aplicar la jurisdicción a una determinada situación en la que por las características, el sujeto activo y el sujeto pasivo se encuentre en diferentes lugares, se podrá utilizar la siguiente teoría:

"Territorial jurisdiction has given rise to two derivative forms of jurisdiction. Subjective territorial jurisdiction involves the application of the law of the Estate exercising jurisdiction to an incident that is initiated within its territory but completed elsewhere. It applies even if the offending cyber activities have no effect within the Estate exercising such jurisdiction over individuals to the State where the particular incident has effect even though the act was initiated outside its territory.

Objective territorial jurisdiction is of particular relevance to cyber operations. For example, in 2007, Estonia was target in cyber operations initiated at least partially from abroad. As to those acts which violated Estonian law, Estonia would at a minimum have been entitled to invoke jurisdiction over individuals, its jurisdiction would have been justified because the operation substantial effects on Estoniant territory, such as interference with the banking system and govermental functions. Similarly, civilians involved in cyber operations against Georgia during that State´s international armed conflict with the Russian Federation in 2008 would have been subject to Georgian jurisdiction on the basis of significant interference with website and disruption of cyber communications in violation of Georgian law"[298]

[297] Google traductor – Del Inglés al Español.
[298] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE. Cambridge University Press, pp. 20.

"La competencia territorial ha dado lugar a dos formas derivadas de la jurisdicción. Competencia subjetiva territorial consiste en la aplicación de la ley del Estado que ejerce la competencia a un incidente que se inicia dentro de su territorio, pero terminó en otro lugar. Se aplica incluso si las actividades de la delincuencia cibernética no tienen ningún efecto en el Estado que ejerce la jurisdicción sobre tales individuos al estado en el incidente particular tiene efecto a pesar de que el acto se inició fuera de su territorio. Competencia Objetiva territorial es de particular importancia para las operaciones cibernéticas. Por ejemplo, en 2007, Estonia fue objetivo en operaciones cibernéticas iniciadas al menos parcialmente desde el exterior. En cuanto a los actos que violan el derecho de Estonia, Estonia podría como mínimo haber podido invocar la jurisdicción sobre los individuos, su jurisdicción habría estado justificada porque las operaciones y efectos sustanciales en el territorio de Estonia, tales como la interferencia con el sistema bancario y funciones Gubernamentales. Del mismo modo, los civiles que participan en las operaciones cibernéticas contra Georgia durante ese conflicto armado internacional, los Estados con la Federación Rusa en 2008 habrían sido sometidos a la jurisdicción de Georgia sobre la base de una interferencia significativa con la página web y la interrupción de las comunicaciones cibernéticas en violación de la ley de Georgia."[299]

Habiendo ya dejado en claro el tema de la jurisdicción en materia de Ciber incidentes, continuaremos describiendo el territorio nacional para comprender los desafíos que la defensa en materia Cibernética implica, ***TOMANDO EN CUENTA QUE EL DESARROLLO DE LAS TECNOLOGÍAS HACE QUE LAS DIFERENTES ACTIVIDADES DEL ESTADO SE DESARROLLEN MÁS Y SE INVOLUCRE CADA VEZ CON LA INTERNET, POR LO QUE SI ALGUNA INFRAESTRUCTURA EN LA REALIDAD NO ES O ERA CONSIDERADA INFRAESTRUCTURA CRITICA, CON EL***

[299] Google traductor – Del Inglés al Español.

DESARROLLO TECNOLÓGICO PUEDE QUE EN EL FUTURO ESA MISMA INFRAESTRUCTURA SE CONVIERTA EN UNA INFRAESTRUCTURA CRITICA CIBERNÉTICA POR EL GRAN TRÁFICO DE INFORMACIÓN QUE GENERA O POR LA RELEVANCIA PARA EL DESARROLLO DE LAS ACTIVIDADES ESTATALES.

Si bien hemos establecido que en materia Cibernética no existen límites físicos, y tampoco el Estado puede ejercer soberanía sobre el Ciber espacio, consideramos que, como ya hemos dichos líneas arriba, que el Estado puede ejercer su soberanía sobre las infraestructuras cibernéticas, pero estas infraestructuras cibernéticas se encuentran dentro de espacio físicos reales los cuales son objeto de protección en la realidad, es por ello que es necesario conocer el territorio, la realidad geo-política, las estadísticas de población, las relaciones con países de la región, los límites fronterizos, entre otros aspectos.

Ubicación en el Continente[300]

- El Perú se encuentra ubicado en la región central y occidental de América del Sur. Limita al norte con Ecuador (1,529 km.) y Colombia (1,506 km.), al este con Brasil (2,822 km.), al sureste con Bolivia (1,047 km.) al sur con Chile (169 km.).

- La frontera con estos cinco países tiene una extensión de 7,073 kilómetros y franquea zonas del país que en su mayoría se ubican en lugares agrestes y de difícil acceso, que constituyen un desafío para el desarrollo e integración. En el oeste se encuentra el Océano Pacífico, el litoral tiene 3,080 kilómetros de extensión y el dominio marítimo se extiende a 200 millas.

- La superficie del Perú incluidas sus islas es la siguiente:
    - Espacio Continental: Área Terrestre: 1'285,215 km2

[300] LIBRO BLANCO DE LA DEFENSA DEL PERÚ (2005) Capitulo II pp.45

- Espacio Marítimo: Mar de Grau, 200 millas de dominio marítimo, a partir del litoral.
- Presencia en la Antártida: el Perú tiene instalada la Base Científica Machu Picchu, ubicada en la Isla Rey Jorge
- El Perú es el tercer país más grande de América del Sur, después de Brasil y Argentina, siendo su capital la ciudad de Lima, principal centro del poder político, comercial y financiero del país.

Características del Territorio[301]

En el Perú se distinguen tres grandes regiones naturales: la costa, la sierra y la selva, ésta última constituida por la selva alta y la selva baja. Cabe destacar que estas regiones naturales, encierran un gran potencial de recursos naturales, que la habilidad y creatividad del hombre peruano han sido históricamente capaz de explotar.

- La Costa, es estrecha y mayormente desértica, con una extensión de 3,080 Km., y cuyo ancho varía entre los 65 y 160 Km. Es atravesado por 52 ríos que forman igual número de valles, que configuran espacios irrigables sumamente productivos. Ocupa el 11% del total de la superficie territorial.
- La Sierra, está conformada por la cordillera de los Andes que es el fenómeno morfológico más importante del Perú por ejercer la mayor influencia en el relieve, el clima, los recursos hídricos, vegetales, animales y minerales del país. Corre paralela a la línea de costa, configurando profundas quebradas, macizos, altiplanicies, llanuras y valles interandinos longitudinales y transversales. La Sierra comprende aproximadamente una tercera parte del país (30%),

[301] Loc. Cit. Ídem.

con un ancho de 400 Km. en el sur y 240 Km. en el norte.

La altitud de la sierra varía de 500 a 6,700 msnm., entre estas cotas se registran distintos pisos ecológicos con climas, flora y fauna diferentes. La cordillera está formada por tres cadenas: la oriental, central y la occidental que se unen y entrecruzan del norte a sur. Este escenario geográfico favoreció el surgimiento de grandes culturas y civilizaciones en el pasado.

- La Selva, es la mayor de las tres regiones y abarca el 59% del territorio del Perú; está cubierta de densos bosques tropicales en el oeste y espesa vegetación en el centro. Es una región en gran parte inexplorada y escasamente poblada.

  La Selva Alta varía entre una altitud de 400 a 1,000 msnm., tiene un relieve irregular y se encuentra en las estribaciones andinas, formando valles de gran fertilidad, también posee una ingente riqueza mineral y potencial energético.[302]

Cuadro de Distribución del Territorio Peruano[303]:

SUPERFICIE DEL TERRITORIO		
	SUPERFICIE en KM	PORCENTAJE % del Total
COSTA	COSTA 136,233	11
SIERRA	SIERRA 391,991	30
SELVA	SELVA 756,991	59
TOTAL	1´285,215	100

*Información actualizada 2005

[302] LIBRO BLANCO DE LA DEFENSA (2005) Capitulo II, pp. 46.
[303] Loc. Cit. Ídem.

Cuencas hidrográficas[304]

El Perú cuenta con cuatro grandes cuencas hidrográficas:

- La Cuenca del Pacífico, comprende 52 ríos paralelos entre sí, que desembocan en el mar;
- La Cuenca del Amazonas, está conformada por las regiones por donde transcurren los ríos que conforman el Amazonas. Este río es navegable durante todo el año por embarcaciones de mediano tonelaje, y permite la salida hacia el Océano Atlántico, materializando la proyección geopolítica bioceánica del Perú.
- La Cuenca del río Madre de Dios, en el sureste del Perú, que es afluente del río Madeira y que, por transporte multimodal, permite el acceso a las rutas del Paraná-Paraguay y su salida al Atlántico por la vía del Río de la Plata en Argentina.
- La Cuenca del Titicaca, compartida con Bolivia, en el lado peruano está formado por los ríos Pucará, Azángaro, Ramis, Chaquimayo, Ilave, y otros. La importancia del Lago Titicaca reside en que atempera la gélidez de la región posibilitando el desarrollo de asentamientos y poblaciones humanas y además, los ríos provenientes del lago, como el Desaguadero son fuentes importantes para la economía de la cuenca.

Lagos

- Existen más de 12,000 lagos y lagunas, el más importante es el Lago Titicaca, uno de los más altos del mundo, está ubicado en la región del Altiplano en la frontera entre Perú y Bolivia, ubicado a 3,800 msnm. Tiene una extensión de 8,710 Km2. correspondiendo al Perú, 5,318 Km2.

[304] Loc. Cit. pp.47

Clima

- El clima en el Perú es sumamente variado, oscilando desde altas temperaturas tropicales en la Selva, hasta muy bajas en la Cordillera de los Andes. El territorio peruano cuenta con 84 "microclimas" de los 114 que existen en el mundo y más del 75% de ecosistemas. Esta situación favorece la biodiversidad en las tres regiones naturales. En el Perú se acumulan más especies de plantas y de animales que en ningún otro lugar del planeta, por ejemplo el 20% del total de aves, entre 40,000 y 50,000 especies de plantas, entre ellas, más de 3,000 tipos de orquídeas.

El Mar

- La presencia de la Cordillera de los Andes y el afloramiento costero de masas de aguas frías proveniente de la Corriente de Humbolt, que se forma como consecuencia de que los vientos alisios provenientes de la costa que arrastran las aguas calientes del mar, haciendo emerger del fondo marino el agua fría, rica en fosfatos y nitratos que sirven de alimento al plancton que a su vez es consumido por peces y otros animales marinos, creando una cadena alimenticia que proporciona la riqueza y variedad biológica que hacen del Mar Peruano, uno de los más ricos del mundo, constituyéndose en fuente de alimentación y de desarrollo industrial.
- Recurrentemente se presenta el fenómeno de "El Niño", motivado por el debilitamiento de los vientos alisios que arrastran las aguas calientes provocando su retorno y concurrentemente, el bloqueo de la Corriente de Humbolt haciendo desaparecer el plancton y los peces. Debido a la temperatura del agua se produce una mayor evaporación, provocando lluvias en la costa, en algunos casos con consecuencias negativas.

La población Peruana[305]

- La población peruana fue estimada al 2005, por el Instituto Nacional de Estadística e Informática (INEI), en de 28 millones 220 mil 764 habitantes. Esta población no se encuentra distribuida de modo homogéneo en el territorio nacional, encontrándose departamentos y provincias con altos índices de concentración poblacional.[306]
- De acuerdo con las últimas estimaciones de población, en el país existen 18 ciudades con más de 200 mil habitantes.[307]
- El Perú tiene una población relativamente joven, ascendiendo a 8 millones 698 mil 780 jóvenes, que comprende de entre cero y catorce años de edad.[308]
- La Población económicamente activa, constituida por el grupo poblacional de 15 a 64 años, conforma por 20 millones 409 mil 515 entre hombres y mujeres de la población. La población de más de 64 años, asciende a 2 millones 043 mil 348 habitantes.[309]
- Con relación a los escenarios demográficos probables para el año 2025, se estiman las siguientes hipótesis[310]:
    - Si la tasa global de fecundidad (hijos por mujer) es de 2,6 la población llegará a un total de 38 millones 179 mil habitantes (hipótesis alta);
    - Si la tasa global de fecundidad es de 2.1 la población será de 35 millones 725 mil personas (hipótesis media-oficial); y
    - Si la tasa global de fecundidad es de 1.6 hijos por mujer, la población alcanzará un total de 33 millones 168 mil habitantes (hipótesis baja).

---

[305] INEI.GOB.PE – Portal del Instituto Nacional de Estadística e Informática, https://www.inei.gob.pe/estadisticas/indice-tematico/poblacion-y-vivienda/, Información sustraída: 27/03/2016.
[306] INEI.GOB.PE – Portal del Instituto Nacional de Estadística e Informática, https://www.inei.gob.pe/estadisticas/indice-tematico/poblacion-y-vivienda/, Información sustraída: 27/03/2016.
[307] Loc. Cit., https://www.inei.gob.pe/estadisticas/indice-tematico/poblacion-y-vivienda/, Información sustraída: 27/03/2016.
[308] Loc. Cit., https://www.inei.gob.pe/estadisticas/indice-tematico/poblacion-y-vivienda/, Información sustraída: 27/03/2016.
[309] Loc. Cit., https://www.inei.gob.pe/estadisticas/indice-tematico/poblacion-y-vivienda/, Información sustraída: 27/03/2016.
[310] LIBRO BLANCO DE LA DEFENSA DEL PERÚ (2005) Capitulo II pp.48

- En términos culturales, el Perú es un país pluricultural y multilingüe; esta característica de origen histórico, plantea al Estado la responsabilidad de lograr la unidad en la pluralidad, respetando las expresiones socioculturales de cada región del país.

Perfil Geoestratégico

- El Perú del 2016, es un país que se ha demostrado que gracias a su abundancia en recursos naturales y a su favorecida ubicación geográfica puede formar parte del gran flujo comercial entre los países de la región así como con los países del resto de mundo, convirtiéndose en un socio estratégico importantes para el acceso al mercado de América del Sur, así como para comercialización de materias primas.
- La nueva realidad Económico-Política del Perú ha hecho posible que retos del pasado se vuelvan realidad en la actualidad, fortaleciendo relaciones con grupos Económicos como APEC, ASPA, la Alianza del Pacifico, UNASUR, entre otros, hacen posible que los países de América del Sur podamos hacer llegar nuestros productos a los 4 extremos del mundo.
- Los desafíos del nuevo mundo tecnológico, hace necesario que el Perú asuma nuevos retos, siguiendo con este proceso de crecimiento, deberá de implementar proceso seguros que faciliten y viabilicen la relación con otros países.

Presencia del Perú en el Pacífico[311]

1. La Cuenca del Pacífico, está conformada por más de sesenta Estados, entre continentales e insulares, con una población creciente que ya supera los 2,000 millones de habitantes, con notable desarrollo económico. En el siglo XXI las emergentes economías del Pacífico lograrán una posición de predominio con sus enormes mercados potenciales.

[311] LIBRO BLANCO DE LA DEFENSA DEL PERÚ (2005) Capitulo II pp.50

Eje del Amazonas[312]

Parte de los puertos de Paita y Bayóvar ubicados en el departamento de Piura, interconecta la región norte del Perú con la región oriente del Brasil, en particular el Estado de Amazonas, cuya capital es Manaos, continuando por navegación fluvial hasta Belem do Pará y Macapá en el Océano Atlántico. Este eje contará además con un ramal central (Callao- Pucallpa- Iquitos) que conecta las regiones del centro del Perú con el resto del Eje.Este eje posibilitará la generación de centros de apoyo logístico y de servicios en nuestros puertos marítimos y fluviales que apoyará la vinculación directa y eficiente del eje con su área de influencia.

En el corto plazo, el Perú exportará fosfatos a Brasil y tiene la posibilidad de abastecer a Manaos con productos alimenticios provenientes de la costa y sierra del Perú.

En una primera etapa se busca consolidar la conexión Paita-Yurimaguas Iquitos-Manaos-Belem Do Pará. La conclusión de esta vía, así como el mejoramiento de la navegación fluvial en los ríos Huallaga, Marañón y Amazonas, potenciará el comercio de nueve Regiones del norte y oriente del Perú que quedarán vinculadas con los Estados Amazonas y Roraima en Brasil. Éstas son: Tumbes, Piura, Lambayeque, La Libertad, Cajamarca, Amazonas, San Martín, Loreto y Ucayali; este eje también promoverá el desarrollo de los puertos de Paita y Bayóvar en el norte del país.

El Estado de Amazonas y toda la cuenca del río Madeira tienen tierras ácidas que necesitan fosfatos, que pueden ser abastecidos por Bayóvar. Manaos, capital del Estado de Amazonas, importa el 80% de los alimentos que consume, necesidad que podrá ser atendida por las nueve Regiones de Perú mencionadas anteriormente, todas ellas productoras de alimentos.

Los Presidentes de Perú y Brasil también han coincidido en la conveniencia de implementar en Iquitos un Centro de Concentración Logística,

[312] Loc. Cit. Ídem.

Transformación y Exportación, que podría reunir la carga destinada a Brasil desde los puertos de Tumaco (Colombia) Esmeraldas, Manta, Guayaquil y Puerto Bolívar (Ecuador), Paita y Bayóvar (Perú) y los puertos fluviales de Saramiriza, Yurimaguas y Pucallpa.

Eje Perú-Brasil-Bolivia[313]

Este Eje vincula a las regiones del sur del Perú con los Estados de Acre y Rondonia de Brasil. Iniciándose en los puertos de Ilo y Matarani, se establecen dos ramales:

1. Matarani-Arequipa-Juliaca-Cusco-Inambari-Puerto Maldonado e Iñapari en la frontera con Brasil, desde donde se dirige a Río Branco y Porto Velho.
2. El segundo ramal comprende: Ilo-Moquegua-Puno e Inambari.

La importancia de este Eje radica en que abre nuevas posibilidades para el desarrollo económico de las regiones del sur del Perú. La producción maderera se verá beneficiada por la disminución de los costos de transporte entre los centros de producción, y los mercados nacionales e internacionales. Asimismo, se hará posible la exportación de producción agrícola e industrial de las regiones del sur del Perú hacia los mercados de Brasil, en condiciones de competitividad, gracias a una infraestructura adecuada.

La implementación de este eje va a favorecer y potenciar el desarrollo de seis Regiones del sur del Perú: Madre de Dios, Cusco, Puno, Arequipa, Moquegua y Tacna.

Eje Interoceánico Central[314]

Este Eje vincula los puertos de Ilo y Matarani del sur del Perú con los Estados de Mato Grosso, Mato Grosso do Sul, Sao Paulo y Río de Janeiro de Brasil. Esta vinculación está intermediada por Bolivia y Paraguay, de allí que sea

[313] LIBRO BLANCO DE LA DEFENSA DEL PERÚ (2005) Capitulo II pp.52
[314] Loc. Cit. Ídem.

importante completar los tramos faltantes de infraestructura en estos países, a fin de permitir la efectiva conexión de las regiones del sur del Perú con el MERCOSUR.

Por nuestra parte, la carretera Ilo-Desaguadero ya está concluida y en operación, ésta vía de 359 kilómetros ha permitido que el tiempo de viaje se reduzca de 17 a 5 horas.

Eje Andino[315]

El Eje Andino en territorio peruano comprende dos vías longitudinales paralelas que corren de Norte a Sur, una es la carretera Panamericana desde Tumbes hasta Tacna, y la otra, comprende dos ramales:

1. La Marginal de la Selva desde el río Canchis (puerto La Balsa) hasta Puerto Maldonado.
2. Longitudinal de la Sierra que comprende Tingo María-Huánuco - Cerro de Pasco - La Oroya - Huancayo - Ayacucho - Abancay - Cusco - Urcos Juliaca - Puno - Desaguadero.

La carretera Panamericana ingresará al Programa de Concesiones Viales, lo que garantizará su conservación adecuada en el largo plazo.

El resto del Eje Andino requiere importantes inversiones y por tanto demandará más tiempo su materialización.

Presencia en la Antártida[316]

El Perú tiene presencia en la Antártida debido a la proyección de sus meridianos hacia el polo sur. El Perú es país adherente al Tratado Antártico desde 1981. En 1983 se creó la Comisión Nacional de Asuntos Antárticos (CONAAN), organismo que conduce la política nacional antártica.

[315] Loc. Cit. pp.53
[316] LIBRO BLANCO DE LA DEFENSA DEL PERÚ (2005) Capitulo II pp.54

Para ser reconocido como Miembro Consultivo del Consejo Antártico, el Perú llevó a cabo las actividades siguientes:

1. Expediciones de reconocimiento de la zona antártica y ejecución de investigaciones científicas aprobadas por el Consejo Consultivo.
2. Construcción de la Estación Científica "Machu Picchu" con tres módulos:
    a. Vivienda, con un área de 210 m2, para 28 personas.
    b. Taller, casa de fuerza, de 92 m2.
    c. Emergencia de 56 m2.

La Estación Antártica Machu Picchu e encuentra ubicada en la ensenada Mackellar de la Isla Rey Jorge, en el extremo norte de la península antártica.

Desde 1988, el Perú ha realizado 15 expediciones científicas con personal de los Ministerios de Energía y Minas y Pesquería, de los Institutos Geofísico y del Mar, y del Consejo Nacional de Ciencia y Tecnología; con apoyo logístico de las Fuerzas Armadas. Las principales investigaciones científicas corresponden a los Programas siguientes: Biología Humana, Oceanografía Física y Química, Biología, Magnetismo Terrestre, Acústica y, Meteorología y Geofísica.

Perfil Geopolítico[317]

El hecho de limitar con cinco países y tener una frontera de 7,073 Kms, la mayor parte de ella en zonas inhóspitas, agrestes, aisladas y despobladas; constituye un reto para las acciones de defensa y desarrollo orientadas a garantizar la soberanía e integridad territorial.

Los países amazónicos tienen problemas similares en su frontera con el Perú, por tal razón se viene fomentando la acción conjunta para afrontar los obstáculos y las amenazas provenientes de factores como la subversión, el narcotráfico, el contrabando, entre otros problemas de seguridad.

[317] Loc. Cit. Ídem.

La interconexión del Perú con cinco cuencas hidrográficas permitirá un intercambio comercial, industrial, científico-tecnológico, cultural y poblacional significativo.

El Perú en el mediano plazo establecerá interconexiones con los países del Atlántico que buscan llegar a la Cuenca del Pacífico, para lo cual deberá atender tales desafíos, brindando facilidades en puertos, aeropuertos, marina mercante, carreteras confiables, seguridad ciudadana, control migratorio, control delincuencial, control del tráfico de armas y narcóticos, etc.

Hoy el Perú se enfrenta al reto del nuevo milenio con una visión estratégica de desarrollo y seguridad, como un país de potencialidades enormes en sus dimensiones marítima, andina, amazónica y proyección geoeconómica bioceánica, con una presencia privilegiada en la Cuenca del Pacífico, fortalecida por su membresía en APEC y su proyección hacia el Continente Antártico. Todo esto obliga a estructurar un Plan de Desarrollo de largo plazo, orientado hacia los mercados internacionales y cuya economía genere valor agregado y se le dote de tecnología y competitividad, apoyado por un Sistema de Seguridad y Defensa.

2. Realidad Jurídica Nacional.

Continuando con el capítulo, debemos comenzar con el análisis jurídico que incumbe a nuestra investigación. Consideramos necesario en el presente capítulos citar a nuestra norma fundamental, la punta de nuestra pirámide de Kelsen[318], nuestra Constitución Política de 1993:

> "Son deberes primordiales del Estado: *DEFENDER LA SOBERANÍA NACIONAL*; garantizar la plena vigencia de los derechos humanos; *PROTEGER A LA POBLACIÓN DE LAS AMENAZAS CONTRA SU SEGURIDAD*; y promover el bienestar general que se fundamenta en la justicia y en el desarrollo integral y equilibrado de la Nación.

[318] Jurista austríaco de origen judío.

> Asimismo, es deber del Estado establecer y ejecutar la política de fronteras y promover la integración, particularmente latinoamericana, así como el desarrollo y la cohesión de las zonas fronterizas, en concordancia con la política exterior."[319]

Utilizando como base para nuestro análisis, lo establecido por la Constitución como un *DEBER DEL ESTADO*, comenzaremos estudiando la política en materia de *DEFENSA* nivel nacional, para ellos estableceremos a través de delimitar su importancia, el porqué es importantes la actualización del *LIBRO BLANCO* de la *DEFENSA NACIONAL*.

- **Libro Blanco de la Defensa Nacional**

En el Perú se publicó en Abril del 2005 la última edición de *LIBRO BLANCO DE LA DEFENSA NACIONAL*, tenido como Presidente de la Republica al Ex Presidente Sr. Alejandro Toledo Manrique y como Ministro de Defensa al Sr. Roberto Chiabra León.

La pregunta básica: *QUE ES EL LIBRO BLANCO DE LA DEFENSA NACIONAL?* Para dar respuesta a esta pregunta utilizaremos las palabras de presentación del Ex Presidente Toledo:

> "…se desarrollan los temas relacionados con la Seguridad y la Defensa Nacional, así como los objetivos y políticas que de ellas se derivan y que los peruanos debemos conocer para que nuestra participación en la Seguridad y la Defensa Nacional, resulte efectiva."[320]

La importancia que tiene un *LIBRO BLANCO* en una realidad como la *Peruana,* es básica, debido a que a través de este documento se va a poder trazar las directrices de lo que va a ser la política en materia de *Defensa.* En

[319] Constitución Política del Perú (1993) Titulo II Capítulo I Art. 44.
[320] Libro Blanco de la Defensa Nacional (2005) Presentación del Libro Blanco de la Defensa Nacional. Pp 03.

Argentina se publicó el *LIBRO BLANCO DE LA DEFENSA* en el año 2014, ellos entienden al *LIBRO BLANCO* de la siguiente manera:

> "El Libro Blanco es un documento oficial a través del cual se presentan los lineamientos fundamentales de la política y del sistema de defensa del país. Su elaboración, y la actualización periódica de su contenido, contribuye al cumplimiento de dos propósitos elementales: por un lado, compromete a la conducción política democrática en un proceso de rendición de cuentas acerca de las características, los objetivos, los medios y las capacidades que posee el sistema de defensa nacional; posibilitando a la ciudadanía el acceso a información clave vinculada a cuánto, cómo y para qué se aplican los recursos públicos que se destinan al sector. Por otro lado, en el plano internacional, la difusión de los lineamientos básicos de la política y la doctrina de defensa nacional implica transparentar el posicionamiento estratégico que adopta el país en el ámbito internacional y regional, evitando de ese modo el surgimiento de percepciones erróneas o distorsionadas que puedan afectar los vínculos de cooperación y confianza mutua entre las naciones, fomentando al mismo tiempo la convivencia pacífica y los principios democráticos de gobierno."[321]

El *LIBRO BLANCO,* tiene entonces dos ámbitos de aplicación, por un lado, *ES LA CONCRETIZACIÓN DE LA POLÍTICA INTERNA QUE VA A DESARROLLAR EL ESTADO EN EL FUTURO CERCANO O HASTA QUE DECIDA CAMBIARLA, ESTABLECIENDO DIRECTRICES, CON METAS Y OBJETIVOS PLANTEADOS A CORTO, MEDIANO Y LARGO PLAZO, ESTABLECIENDO LOS MEDIOS Y RECURSOS DEL SISTEMA DE DEFENSA* (Ámbito Interno)[322], *Y POR OTRO LADO EL LIBRO BLANCO EXPONE LOS LINEAMIENTO DE LA POLÍTICA DE DEFENSA COADYUVANDO AL POSICIONAMIENTO ESTRATÉGICO EN EL*

[321] MINDEF.GOB.AR – Portal del Ministerio de Defensa de Argentina, Libro Blanco de la Defensa, http://www.mindef.gov.ar/index.php
[322] Concepto del Tesista.

PLANO INTERNACIONAL, TRANSPARENTANDO LA DOCTRINA DE DEFENSA DEL PAÍS (Ámbito Externo)[323].

Para seguir confirmando la importancia de la creación o actualización del *LIBRO BLANCO,* utilizaremos la experiencia francesa, a través del discurso de presentación del *LIBRO BLANCO* por parte del *PRESIDENTE FRANCOIS HOLLANDE*:

> "J'ai en effet considéré que l'état du monde appelait de nouvelles évolutions stratégiques. Qui ne voit que le contexte a sensiblement changé depuis 2008?"[324]
>
> "Ciertamente he visto el estado del mundo hace un llamado a nuevos desarrollos estratégicos. ¿Quién no ve que el contexto ha cambiado significativamente desde 2008?"[325]

En definitiva, sí para un país como Francia la realidad ha cambiado, para un país como el Perú podrá haber cambiado desde el 2005? En definitiva la respuesta es AFIRMATIVA, si bien Francia es un país con un desarrollo superior al Perú, eso no da lugar para desmerecerlo, el Perú se ha desarrollado mucho en estos últimos 10 años, es por ello que se hace necesario hacer la peruanización de la pregunta que se hizo el *PRESIDENTE HOLLANDE:* Qui ne voit que le contexte a sensiblement changé depuis 2005? - ¿Quién no ve que el contexto ha cambiado significativamente desde 2005?

- **Ley de Protección de Datos Personales**

Debemos entender que para el presente punto, la Norma Jurídica, es una herramienta y no un fin, la implementación de normas acorde a la realidad internacional, ya habiendo demostrado que el Perú cuenta con experiencias en ciberataques, hará que el Perú evolucione sus acciones para poder afrontar de mejor manera situaciones en las que se vulnere la seguridad a la

---

[323] Concepto del Tesista.
[324] LELIVREBLANCDELADEFENSEETSECURITE.GOUV.FR – Portal del Libro Blanco de Defensa y la Seguridad, http://www.livreblancdefenseetsecurite.gouv.fr/pdf/le_livre_blanc_de_la_defense_2013.pdf, pp.7, Información sustraída: 25/03/2016
[325] Google traductor – Del Francés al Español.

soberanía así como la seguridad de sus habitantes, recordando que es, según la *CONSTITUCION POLITICA,* el fin supremo del Estado.

El análisis jurídico lleva consigo que analicemos todas las normas que el Estado Peruano a emitido en favor de la ciberseguridad y la ciberdefensa, para ellos la primera normal en mención es sobre la *PROTECCION DE DATOS PERSONALES,* la Ley de Protección de Datos Personales, es una herramienta trabajada por el Ministerio de Justicia y se basa en el artículo 2, numeral 6 de la Constitución Política del Perú de 1993, que a la letra dice:

> "Toda persona tiene derecho a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten a la intimidad personal y familiar."[326]

Un derecho Constitucionalmente reconocido, se hace necesario que sea protegido con especial celo por el Estado y reglamente a los actores que participan dentro de las posibles futuras relaciones, en este caso específico, es más un hecho que una posibilidad, debido a que actualmente todos los datos recopilados por los agentes autorizados tiene como fuente los sistemas informáticos.

La Protección de Datos Personales está relacionada con: "*el derecho que tiene toda persona a controlar la información que comparte con terceros, así como el derecho a que esta información se utilice de forma apropiada, es decir, que no la perjudique"*[327]

Lo que se busca reglamentar es al proveedor del servicio de almacenamiento, y a su *BANCO DE DATOS PERSONALES*, entonces es necesario hacernos la siguiente pregunta: ¿QUE ES UN BANCO DE DATOS PERSONALES?

> "Es el conjunto organizado de datos personales, automatizado o no, independiente del soporte en que se encuentren, sea este físico, magnético, digital, óptico u

[326] Constitución Política del Perú, articulo 2, inciso 6.
[327] AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS PERSONALES, Ministerio de Justicia, Guía de Inscripción de Bancos de Datos Personales pp 6.

> otros que se creen, cualquiera fuera la forma o modalidad de su creación, formación, almacenamiento, organización y acceso."

DESDE NUESTRO PUNTO DE VISTA, EL PRESENTE CONCEPTO SE ENCUENTRA ACORDE A LA REALIDAD, ESTO DEBIDO A QUE NO CIERRA EL CONCEPTO, SINO MÁS BIEN LO DEJA LO SUFICIENTEMENTE ABIERTO COMO PARA QUE SI EN EL FUTURO SE CREA OTRO MECANISMO PARA EL ALMACENAMIENTO DE DATOS, EL ORDENAMIENTO NO TENGA QUE CAMBIAR, SI NO DE INMEDIATAMENTE SEA RECONOCIDO Y SE LE APLIQUEN LAS MISMA REGLAS QUE, ENTENDIENDO QUE, PARA ESTE CASO EN PARTICULAR, EL FIN ES EL ALMACENAMIENTO DE DATOS LOS MEDIOS PUEDEN VARIAR, PERO OBJETIVO NO.

Sabiendo ya que son los *BANCOS DE DATOS PERSONALES*, ahora es necesario saber ¿Qué SON LOS DATOS PERSONALES?

> "La Ley de Protección de Datos Personales se aplica a los datos personales contenidos o destinados a ser contenidos en bancos de datos personales privados o públicos cuyo tratamiento se realiza en el territorio nacional"[328]

La excepción a esta regla serian *BANCOS DE DATOS PERSONALES* creados por personas naturales para una actividad exclusivamente privada o familiar y los *BANCOS DE DATOS* administración publica creados para el cumplimiento de funciones asignadas por ley para la defensa nacional, seguridad pública y para el desarrollo de actividades en materia penal para la investigación y represión del delito.[329]

Según esta nueva *LEY DE PROTECCION DE DATOS PERSONALES* que datos son sensibles?

[328] AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS PERSONALES, Ministerio de Justicia, Guía de Inscripción de Bancos de Datos Personales pp 6.
[329] Loc. Cit. pp 7.

- Los datos biométricos, debido a que pueden identificar a una persona, por ejemplo: la huella digital, la retina, el iris.
- Datos referidos al origen racial y étnico.
- Ingresos económicos.
- Opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical.
- Información relacionada a la salud o a la vida sexual.

Continuando con la *LEY DE PROTECCIÓN DE DATOS PERSONALES (Ley 29733)*, a través de la cual se crea o mejor dicho se le designa al *MINISTERIO DE JUSTICIA*, específicamente a la *DIRECCIÓN NACIONAL DE JUSTICIA* como la *AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS PERSONALES*, con posterioridad, en el año 2012 se aprueba el *REGLAMENTO DE ORGANIZACIÓN Y FUNCIONES* del *MINISTERIO DE JUSTICIA Y DERECHO HUMANOS,* en donde se creó un órgano denominado *DIRECCION GENERAL DE PROTECCION DE DATOS PERSONALES,* adscrito al *DESPACHO VICEMINISTERIAL DE DERECHO HUMANOS Y ACCESO A LA JUSTICIA,* y este es denominado ***AUTORIDAD NACIONAL DE PROTECCION DE DATOS PERSONALES.***

- ***Autoridad Nacional de Protección de Datos Personales***

RESULTA ENTONCES NECESARIO REGLAMENTAR O PROTEGER LOS DATOS PERSONALES? Pues si, por las siguientes razones:

- Se puede obtener información personales de todo tipo, como ubicación, familiares, grupo social, lugares de preferencia.
- Es posible acceder a información financiera de los usuarios de la *INTERNET.*
- Se puede obtener información detallada de los bienes de los usuarios de la *INTERNET.*
- Es necesario proteger la confianza de los usuarios de la *INTERNET.*

Los Datos Personales, entendido como la información privada de todos los Peruanos, puede ser tomada como una posible infraestructura critica*,* debido a que a través de esta información los cibercriminales puede realizar acciones

delictivas, que para los efectos de la presente ley, no hace más que mellar en la conciencia del usuario que a fin de cuentas es el principal actor dentro de la internet y esto tiene un repercusión directa en el mercado, porque es en base a la confianza que la internet continua desarrollándose.

La presente Ley (29733) establece los siguientes conceptos, mencionaremos algunos aspectos:

- Datos Personales.- Toda información sobre una persona natural que la identifican o la hace identificable a través de medios que pueden ser razonablemente utilizados. [330]
- Datos sensibles.- Datos personales constituidos por los datos biométricos que por si mismos pueden identificar al titular; datos referidos al origen racial y étnico, ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales, afiliación sindical, e información relacionada a la salud o a la vida sexual.[331]
- Flujo transfronterizo.- Transferencia internacional de datos personales a un destinatario situado en un país distinto al país de origen de los datos personales, sin importar el soporte en que estos se encuentre, los medios por los cuales se efectuó la transferencia ni el tratamiento que reciban.[332]
- Nivel suficiente de protección para los datos personales.- Nivel de protección que abarca por lo menos la consignación y el respeto de los principios rectores de esta ley, así como medidas técnicas de seguridad y confidencialidad, apropiadas según la categoría de datos de que se trate.[333]
- Procedimiento de anonimización.- Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es irreversible.[334]
- Procedimiento de disociación.- Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es reversible.[335]

[330]LEY DE PROTECCIÓN DE DATOS PERSONALES, LEY N°29733, art. 2 numeral 4.
[331] Loc. Cit., art. 2 numeral 5.
[332] Loc. Cit., art. 2 numeral 8.
[333] Loc. Cit., art. 2 numeral 10.
[334] Loc. Cit., art. 2 numeral 12.

La Ley de Protección de Datos Personales, introduce un estándar mínimo de protección a través de la conceptualización de los términos empleados para la material, entre ellos captan nuestra especial atención términos como: *DATOS SENSIBLES, FLUJO TRANSFRONTERIZO, NIVEL SUFICIENTE DE PROTECCION PARA LOS DATOS PERSONALES,* consideramos que al introducir un estándar mínimo, la realidad jurídica del servicio mejora, pero esta actividad de hombre solo se verá favorecida en la medida que los mecanismo de fiscalización sean los adecuados, para ello no es necesario únicamente normar la realidad sino implementar medidas de control en la realidad, es por ello que consideramos *QUE LA BIPOLARIDAD DE LO CIBER HACE NECESARIO QUE EL ESTADO REALICE DOS TIPOS DE ACCIONES, POR UN LADO LA DE REGULAR DE MANERA DIRECTA Y PRACMATICA LA REALIDAD; E IMPLEMENTE MEDIDAS DE CONTROL AGRESIVAS CON CAPACIDAD DE REACCION ANTE LA POSIBLE EVOLUCION DE MANERA INMEDIATA.*

OTRO ASPECTO QUE CAPTA NUESTRA ATENCIÓN VA CON RESPECTO A LOS LLAMADOS PRINCIPIOS RECTORES QUE PROCLAMA LA PRESENTE LEY, EN DEFINITIVA CONSIDERAMOS QUE EL HECHO DE POSITIVIZAR[336] *CONDUCTAS QUE SE ENCUENTRAN EN EVOLUCIÓN CONSTANTE NO RESULTA ADECUADO, HACE QUE EL ORDENAMIENTO GASTE RECURSO Y ESFUERZOS EN MEJORAR O ADECUAR SU ORDENAMIENTO POR CADA CAMBIO, EN TAL SENTIDO NOS ENCONTRAMOS DE ACUERDO CON RESPECTO QUE SEAN LOS PRINCIPIOS LOS QUE ESTABLEZCAN CONDUCTAS PUNIBLES, ENTENDIENDO QUE LOS PRINCIPIOS TIENEN UN ÁMBITO DE APLICACIÓN MÁS AMPLIO A COMPARACIÓN DE UN ARTÍCULO QUE POSITIVIZA UNA CONDUCTA DETERMINADA, ASÍ MISMO CONSIDERAMOS QUE UNA RAMA DEL DERECHO COMO LO CIBERNETICO NO ES POSIBLE REGULARLA O POSITIVIZARLA A TRAVÉS DE PRINCIPIOS, SINO ADEMÁS ES*

---

[335] Loc. Cit., art. 2 numeral 13

[336] POSITIVIZAR.- El **derecho positivo** es el conjunto de normas jurídicas escritas por una soberanía, esto es, toda la creación jurídica del órgano estatal que ejerza la función legislativa. El derecho positivo puede ser de aplicación vigente o no vigente, dependiendo si la norma rige para una población determinada, o la norma ya ha sido derogada por la promulgación de una posterior. No sólo se considera derecho positivo a la Ley, sino además a toda norma jurídica que se encuentre escrita

NECESARIO QUE LA POSITIVIZACIÓN SEA ACORDE, NORMANDO O REGULANDO NO ACCIONES SINO RESULTADOS, COMO YA HEMOS DICHO.

- **Ley de Delitos Informáticos – 30096**

La presente Ley introduce la comisión de *DELITOS INFORMATICOS* a nuestro ordenamiento, Código Penal, a través de la cual de intenta *POSITIVIZAR* las posibles conductas dentro del campo *INFORMATICO,* que como ya hemos mencionado líneas arriba: *SEGURIDAD INFORMÁTICA RESPONDE A LA SEGURIDAD QUE DEBEN DE TENER LOS SISTEMAS DE INFORMACIÓN O SISTEMAS INFORMÁTICOS, LA SEGURIDAD DE LA INFORMACION, RESPONDE A LA SEGURIDAD DE LOS DATOS TRANSMITIDOS.*

Según el Dr. Felipe Villavicencio Terreros, las principales características de vulnerabilidad[337] en el mundo informático son:

1. La falta de jerarquía en la red, que permite establecer sistemas de control, lo que dificulta la verificación de la información que circula por este medio.
2. El creciente número de usuarios, y la facilidad de acceso al medio tecnológico.
3. El anonimato de los cibernautas que dificulta su persecución tras la comisión de un delito a través de este medio.
4. La facilidad de acceso a la información para alterar datos, destruir sistemas informáticos.

En definitiva los *DELITOS INFORMATICOS* son un aspecto primordial en materia de *CIBERSEGURIDAD*, y es necesario que el *ESTADO* preste la debida atención además de los expuesto por el Dr. *V*illavicencio, se tiene que tomar en cuenta: "*Otro factor determinante es la rápida difusión de información a través de este medio tecnológico a muy bajo costo que permite a las organizaciones delictivas perpetrar delitos con mayor facilidad."*[338]

[337] VILLAVICENCIO TERREROS, Felipe – Delitos informáticos en la Ley 30096 y la modificación de la Ley 30071, pp. 3

[338] Video: CARNEVALI RODRÍGUEZ, Raúl; "La criminalidad organizada. Una aproximación al derecho penal italiano, en particular la responsabilidad de las personas jurídicas y la confiscación", Vol. 16, Ius Et Praxis Nº 2, Talca, 2010, pág. 273.

Antes de pasar a describir la norma, comentaremos algunos conceptos en lo que a *DELITOS INFORMATICOS*[339] corresponde.

Según *VILLAVICENCIO TERREROS:*

> *"Los delitos informáticos se vinculan con la idea de la comisión del crimen a través del empleo de la computadora, internet, etc.; sin embargo esta forma de criminalidad no solo se comete a través de estos medios, pues éstos son solo instrumentos que facilitan pero no determinan la comisión de estos delitos. Esta denominación, es poco usada en las legislaciones penales; no obstante bajo ella se describe una nueva forma de criminalidad desarrollada a partir del elevado uso de la tecnología informática."*[340]

En este punto consideramos necesario cerrar la diferencia entre *INFORMATICO* y *CIBERNETICO*, si bien a lo largo de la presente investigación hemos usado de manera indistinta ambos términos, de hace necesario para entender el sentido de la *NORMA* establecer bien la diferencia entre ambos términos.

INFORMATICO.- Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de computadoras.[341]

CIBERNETICO.- Ciencia que estudia las analogías entre los sistemas de control y comunicación de los seres vivos y los de las maquinas.[342]

---

[339] Debido al desarrollo de la tecnología y entre ellos la computadora, y dado la nueva forma de comisión de delitos a través de las tecnologías es que se ha optado por denominar indistintamente a este tipo de delitos como "delito de abuso de computadoras", "delitos bajo la influencia de la computadora", "criminalidad de la información y la comunicación", "criminalidad de internet", "criminalidad multimedia", y en el Perú se denomina "delitos informáticos". Todo estas denominación identifican de manera general la problemática de la delincuencia mediante las computadoras y el empleo de las comunicaciones; sin embargo, para efectos didáctico en la doctrina se prefiere la denominación de "delitos informáticos" para identificar la criminalidad vinculada a la tecnología; Vide. MAZUELOS COELLO, Julio F.; "Modelos de imputación en el derecho penal informático", pág. 40.

[340] VILLAVICENCIO TERREROS, Felipe – Delitos informáticos en la Ley 30096 y la modificación de la Ley 30071, pp. 3

[341] RAE.ES – Portal de la Real Academia de la Lengua Española.

Resulta evidente que definir los términos de acuerdo a su significado no es lo mas apropiado para establecer la diferencia y definir cada uno de ellos. Podríamos definir *INFORMATICO* como *CIENCIA ESTUDIA EL ALMACENAMIENTO DE INFORMACION EN EQUIPOS ELECTRONICOS O AUTOMATIZADOS, UTILIZADOS PARA ADMINISTRAR*[343]*,* por otro lado podríamos definir *CIBERNETICO* como *CIENCIA MATEMATICA QUE ESTUDIA LA RELACION ENTRE LOS SISTEMAS ELECTRONICOS.*[344]

Es necesario hacernos la siguiente pregunta: *EXITEN DIFERENCIAS ENTRE DELITO INFORMATICO Y DELITO CIBERNETICO?* Desde nuestro punto de vista, *SI*, mientras que *DELITO INFORMATICO* tiene como objetivo obtener información de algún sistema informático utilizando cualquiera de los mecanismos para acceder a esta información, el *DELITO CIBERNETICO* tiene como objetivo la búsqueda de vulnerabilidades en un sistema informático, como se puede apreciar la línea que los separa es delgada, debido a que a través del *DELITO CIBERNETICO* podríamos encontrar una vulnerabilidad en el sistema informático y así cometer un *DELITO INFORMATICO* sustrayendo la información que buscamos, podríamos encontrarnos con una figura que en el *DERECHO PENAL PERUANO* es conocida como el *CONCURSO REAL DE DELITOS*[345]

Volviendo a la Ley 30096 materias de análisis, consideramos que al igual que la Ley de Protección de Datos Personales, la presente Ley es un intento más del Perú por proteger la confianza del usuario en la internet*, LOS SISTEMAS INFORMATICOS* y *LOS SISTEMAS CIBERNETICOS.*
Por ejemplo los artículos 2, 3 y 4 que a la letra dicen:

- **Artículo 2. Acceso ilícito –** El que accede si autorización a todo o parte de una sistema informático, siempre que realice con vulneración

[342] Loc. Cit.– Portal de la Real Academia de la Lengua Española.
[343] Concepto del Tesista.
[344] Concepto del Tesista.
[345] **Artículo 50.- Concurso real de delitos -** Cuando concurran varios hechos punibles que deban considerarse como otros tantos delitos independientes, se sumarán las penas privativas de libertad que fije el juez para cada uno de ellos hasta un máximo del doble de la pena del delito más grave, no pudiendo exceder de 35 años. Si alguno de estos delitos se encuentra reprimido con cadena perpetua se aplicará únicamente ésta

de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menos de uno ni mayor de cuatro años y con treinta a noventa días multa

Será reprimido con la misma pena el que accede a un sistema informático excediendo lo autorizado.[346]

- **Artículo 3. Atentado contra la integridad de datos informáticos -** El que, a través de1las tecnologías de la información o de la comunicación, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.[347]

- **Artículo 4. Atentado contra la integridad de sistemas informáticos** - El que, a través de las tecnologías de la información o de la comunicación, inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.[348]

- **Artículo 6. Tráfico ilegal de datos** - El que crea, ingresa o utiliza indebidamente una base de datos sobre una persona natural o jurídica, identificada o identificable, para comercializar, traficar, vender,

[346] Información sustraída de: http://www.peru.gob.pe/docs/PLANES/10434/PLAN_10434_2013_Ley_N%C2%B0_30096-DELITOS_INFORMATICOS.pdf – Fecha: 02/04/2016
[347] Información sustraída de: http://www.peru.gob.pe/docs/PLANES/10434/PLAN_10434_2013_Ley_N%C2%B0_30096-DELITOS_INFORMATICOS.pdf – Fecha: 02/04/2016
[348] Información sustraída de: http://www.peru.gob.pe/docs/PLANES/10434/PLAN_10434_2013_Ley_N%C2%B0_30096-DELITOS_INFORMATICOS.pdf – Fecha: 02/04/2016

promover, favorecer o facilitar información relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análoga, creando o no perjuicio, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.[349]

- **Artículo 7. Interceptación de datos informáticos -** El que, a través de las tecnologías de la información o de la comunicación, intercepta datos informáticos en transmisiones no públicas, dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años.

  La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con las normas de la materia.

  La pena privativa de libertad será no menor de ocho ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la soberanía nacionales.[350]

- **Artículo 8. Fraude informático** - El que, a través de las tecnologías de la información o de la comunicación, procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una

[349] Información sustraída de: http://www.peru.gob.pe/docs/PLANES/10434/PLAN_10434_2013_Ley_N%C2%B0_30096-DELITOS_INFORMATICOS.pdf – Fecha: 02/04/2016

[350] Información sustraída de: http://www.peru.gob.pe/docs/PLANES/10434/PLAN_10434_2013_Ley_N%C2%B0_30096-DELITOS_INFORMATICOS.pdf – Fecha: 02/04/2016

pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días multa.

La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social.[351]

- **Artículo 9. Suplantación de identidad** - El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.[352]

Consideramos que los artículos de la ley de Delitos informáticos, son muestra de una realidad en la que se buscaba introducir esta nueva modalidad de delitos en nuestra realidad, bien podríamos relacionar los artículos citados con la *LEY DE PROTECCION DE DATOS PERSONALES*, como mecanismos que buscan proteger la confianza ante posibles situaciones, es un intento por parte del *ESTADO PERUANO* por tipificar la acción de los *DELINCUENTES INFORMATICOS*.

Pero como ya hemos mencionado lo que implica un delito informático es que una individuo con habilidades especiales sustraiga información de personas o entidades para su provecho, pero esto no es lo único que debería tipificarse, ya hemos establecido la diferencia entre el termino informático y el termino cibernético, en ambos casos afectarlos debería ser considerado un delito o la tentativa de la comisión de uno, esto debido a que la sustracción de información seria el hecho punible objetivo, mientras que afectar las vulnerabilidades cibernéticas son el medio para obtener un fin, como el sustraer información.

---

[351] Información sustraída de: http://www.peru.gob.pe/docs/PLANES/10434/PLAN_10434_2013_Ley_N%C2%B0_30096-DELITOS_INFORMATICOS.pdf – Fecha: 02/04/2016

[352] Información sustraída de: http://www.peru.gob.pe/docs/PLANES/10434/PLAN_10434_2013_Ley_N%C2%B0_30096-DELITOS_INFORMATICOS.pdf – Fecha: 02/04/2016

La pobre realidad jurídica, sumada a la falta de promoción de este sector hace que las vulnerabilidades sean más sencillas de explotar.

QUINTO CAPITULO

PROPUESTAS Y RECOMENDACIONES

El presente capítulo tiene como objetivo mostrar las diferentes experiencias de los países desarrollados en matera de *CIBERSEGURIDAD* y *CIBERDEFENSA,* para que de esta forma sean tomadas por el Perú para mejorar la seguridad en materia *CIBERNETICA* e *INFORMATICA*.

Comenzaremos la presente sección utilizando la experiencia Colombiana, en materia de *CIBERSEGURIDAD* y *CIBERDEFENSA*:

> *"…es necesario que los diferentes actores de la sociedad, la Academia, la Empresa y el Gobierno, orienten esfuerzos a la generación de proyectos, iniciativas y planteamientos innovadores de política y normatividad pública enfocados en fortalecer la posición del país en términos de gestión de seguridad de la información, definición y aseguramiento de infraestructura crítica, el mantenimiento de ambientes seguros, el aseguramiento de sistemas y la definición de niveles mínimos suficientes para controlar los riesgos y amenazas de naturaleza cibernética, así como las medidas estratégicas para la gestión de la ciberseguridad, y la configuración de un entorno político adecuado para la implementación de medidas para asegurar al Estado en el ciberespacio, pues es necesario apalancar estas nuevas necesidades desde el punto de vista legislativo, donde los mecanismos de control y de vigilancia son fundamentales para garantizar la estabilidad de las instituciones y la consecución de los objetivos estratégicos del Estado,*

potenciando así la transparencia, la oportunidad, y la optimización de recursos."[353]

Es necesario partir de un punto, y en Colombia ya se están desarrollando herramientas que se utilizaran para mitigar estas actividades que a pesar de darse en un ambiente virtual afectan en la realidad en más de un aspecto a todos, es por ellos que Colombia establece algunos vectores de innovación, como los siguientes:

"A. Generación de políticas, directrices, normas, actos administrativos y otras formas jurídicas que dictaminen las formas, tanto tecnológicas como procedimentales, de llevar a cabo el intercambio de información entre las diferentes entidades del Estado, entre el Gobierno y los diferentes sectores productivos del país y entre la ciudadanía en general, bajo esquemas que garanticen la integridad, la confidencialidad y la disponibilidad de la información.

B. Generación de políticas, normas, actos administrativos, procedimientos legislativos y otras figuras jurídicas orientadas a fortalecer las capacidades y la organización del Estado colombiano para proteger al ciberespacio de amenazas que atenten contra la soberanía nacional y los principios constitucionales.

C. Incorporación de los delitos cibernéticos como elemento fundamental de las políticas, normas, actos administrativos y otras figuras jurídicas, con el fin de fortalecer al Estado en su capacidad para identificar, reconocer y juzgar de manera adecuada estos

[353] Ministerio de Tecnología de la Información y las Comunicaciones, Agenda estratégica de Innovación: Ciberseguridad (2014) pp. 6.

elementos en los procesos jurídicos, constitucionales, penales, etc., definiendo también los alcances, los niveles de gravedad, las penalidades y los procedimientos necesarios ante la ocurrencia de los mismos.

D. Generación de directrices de protección de la confidencialidad, integridad y disponibilidad de los datos del Estado Colombiano durante el ciclo de vida de los mismos, a través de la definición, adopción, ajuste, actualización, incorporación, implementación y valoración de esquemas tecnológicos y procedimentales específicos.

E. Dimensionamiento de políticas de seguridad de la información y ciberseguridad para la incorporación de software en las entidades del Estado, así como para su gestión, dirección, monitoreo, mantenimiento y control, considerando esquemas técnicos, procedimentales, metodológicos y de política nacional.

F. Generación de políticas, normas, actos administrativos, procedimientos legislativos y otras figuras jurídicas orientadas a fortalecer las alianzas y los acuerdos de cooperación y colaboración internacionales de lucha contra amenazas y delitos de naturaleza cibernética, así como aquellos orientados a fortalecer la defensa nacional en el ciberespacio.

G. Estructuración de circulares, políticas, normas, actos administrativos y otras figuras enfocadas a fortalecer las capacidades del Estado para garantizar la adecuada identificación/autenticación, autorización de

los ciudadanos colombianos, así como protección de la identidad de los mismos."[354]

Si bien Colombia, con esta directiva no logra frenar los *CIBERINCIDENTES*, ellos a través de estas directivas logren crear un ordenamiento solido desde la base, reconociendo al ámbito *CIBERNETICO* como una necesidad de atención por parte del *ESTADO*. Como bien lo dice, generar políticas, normas, actos administrativos, procedimientos legislativos y otras figuras jurídicas, es necesario he imperativo para poder comenzar a desarrollarnos en este tipo de actividades.

Por otro lado Argentina, en Noviembre del 2015, inauguró el *CENTRO DE CIBERDEFENSA*, convirtiéndose en un país más de la región que presta atención a lo *CIBERNETICO,* el ministro de Defensa, el Sr. Agustin Rossi, manifestó:

"Es un eje estratégico en la política de Defensa, un desafío enorme que es necesario jerarquizar"[355].

Así mismo manifestó:

"Fortalecer esta nueva dimensión de la Defensa con una mirada integral y multidisciplinaria con la atención puesta en las nuevas tecnologías, participación necesaria del sector empresarial y académico para obtener resultados más eficientes y productivos"[356].

En definitiva el avance en materia de *CIBERDEFENSA* por parte de Argentina es algo que consideramos se deba copiar, somos de la idea que es algo que se debe de *ADAPTAR* a nuestra realidad y utilizar la idea de implementar un sistema que sirva contra *CIBERINCIDENTES.*

---

[354] Ministerio de Tecnología de la Información y las Comunicaciones, Agenda estratégica de Innovación: Ciberseguridad (2014) pp. 8.
[355] MINISTERIO DE DEFENSA ARGENTINA – Portal de Ministerio de Defensa de Argentina, http://www.mindef.gov.ar/plantillaNoticia.php?notId=33, Información sustraída: 24/04/2016
[356] Ob. cit, http://www.mindef.gov.ar/plantillaNoticia.php?notId=33, Información sustraída: 24/04/2016

Por otro lado, El Director General de Ciberdefensa, de Argentina, explico:

> "Se ha venido trabajando en seis ejes fundamentales para el desarrollo de la capacidad: Protección de Infraestructuras Críticas, Investigación y Desarrollo, Capacitación, Vinculación y Difusión, Trabajo Conjunto con las FFAA y Cooperación Internacional"[357].

Se entiende a través de este último mensaje que desarrollar este tipo de tecnologías, no compete a un solo sector, es necesario que la implementación de herramientas en materia de *CIBERSEGURIDAD* y *CIBERDEFENSA* se realice a través de mecanismos multidisciplinarios, involucrando los diversos sectores del *ESTADO*, así como al sector privado.
Continúa el Director General de Ciberdefensa:

> "En materia de vinculación se continúan concretando convenios de cooperación con universidades públicas y cámaras empresarias de tecnología, propiciando el desarrollo de una industria nacional para la ciberdefensa y también en materia de Cooperación Internacional se han firmado actas acuerdos de cooperación con Brasil, Bolivia y Paraguay, intercambiando de esta manera información de experiencias y procurando un abordaje común de la temática"[358]

¿PERO CUALES SERIAN LAS FUNCIONES DE COMANDO DE CIBERDEFENSA? Con respecto a la experiencia Argentina, seria las siguientes:

> *"1.- Asistir en el planeamiento, diseño y elaboración de la política de ciberdefensa de acuerdo a lo establecido en el Ciclo de Planeamiento de la Defensa Nacional en coordinación con la SUBSECRETARÍA DE PLANEAMIENTO ESTRATÉGICO Y POLÍTICA MILITAR.*

[357] MINISTERIO DE DEFENSA ARGENTINA – Portal de Ministerio de Defensa de Argentina, http://www.mindef.gov.ar/plantillaNoticia.php?notId=33, Información sustraída: 24/04/2016
[358] Ob. cit, http://www.mindef.gov.ar/plantillaNoticia.php?notId=33, Información sustraída: 24/04/2016

2.- Entender en la coordinación con los organismos y autoridades de los distintos poderes del Estado para contribuir desde la Jurisdicción a la política nacional de ciberseguridad y de protección de infraestructura crítica.

3.- Intervenir en la orientación, dirección y supervisión de las acciones en materia de ciberdefensa ejecutadas por el Nivel Estratégico Militar.

4.- Ejercer el control funcional sobre el COMANDO CONJUNTO DE CIBERDEFENSA de las FUERZAS ARMADAS.

5.- Intervenir en la evaluación y aprobación de los planes militares de desarrollo de capacidades de ciberdefensa, en la doctrina básica y en las publicaciones militares pertinentes, cualquiera sea su naturaleza.

6.- Intervenir en el diseño de políticas, normas y procedimientos destinados a garantizar la seguridad de la información y a coordinar e integrar los centros de respuesta ante emergencias teleinformáticas.

7.- Fomentar políticas de convocatoria, captación, incentivo y formación de recursos humanos para la ciberdefensa para mantener un plantel adecuado.

8.- Promover vínculos sistemáticos de intercambio y cooperación en materia de ciberdefensa con los ámbitos académico, científico y empresarial.

9.- Impulsar acuerdos de cooperación e intercambio en materia de investigación y asistencia técnica en ciberdefensa con organismos públicos y privados.

10.- Asistir en el desarrollo doctrinario, en el diseño y fortalecimiento de capacidades y en la elaboración de la estrategia de ciberdefensa de conformidad a los lineamientos del Ciclo de Planeamiento de la Defensa Nacional."[359]

Aterrizando en nuestra realidad, lo más cercano al Comando en *CIBERDEFENSA* Argentino, es el *PECERT*, y este se define como:

"Pe-CERT, es el Sistema de Coordinación de la Administración
Publica, creado por RM 360-2009-PCM y es el encargado de liderar los esfuerzos para resolver, anticipar y enfrentar los Ciber Desafíos y coordinar la defensa ante los Ciber ataques, con el fin de proveer a la Nación de una postura Segura en el Ámbito de la Seguridad Informática."[360]

Y tiene como Objetivos:

*"**Promover** la Coordinación entre las entidades de la administración Pública Nacional, para la prevención, detección, detención, manejo y recopilación de información y desarrollo de soluciones para incidentes de seguridad.*

***Coordinar**, colaborar y proponer normas destinadas a incrementar los niveles de seguridad en los recursos y sistemas relacionados con Tecnologías Informáticas de la Administración Publica.*

[359] MINISTERIO DE DEFENSA ARGENTINA – Portal de Ministerio de Defensa de Argentina, http://www.mindef.gov.ar/plantillaNoticia.php?notId=33, Información sustraída: 24/04/2016
[360] PECERT.COM – Portal del PeCert, http://www.pecert.gob.pe/pecert-acerca-de.html, Información sustraída: 24/04/2016

Asesorar *Técnicamente ante incidentes de seguridad en los sistemas informáticos que reporten los distintos organismos de la Administración Publica Nacional.*

Asesorar *a los organismos de la Administración Publica Nacional Sobre las herramientas y Técnicas de protección y defensa de sus sistemas de Información.*

Centralizar *los Reportes sobre incidentes de seguridad ocurridos en redes teleinformáticas de la Administración pública Nacional y facilitar el intercambio de la información para afrontarlos.*

Actuar *como repositorio de toda la información sobre incidentes de seguridad, herramientas, técnicas de protección y defensa.*

Difundir *información útil para incrementar los niveles de seguridad de las redes teleinformáticas de la Administración Pública Nacional.*

Interactuar *con Coordinaciones de Similar Naturaleza."*[361]

De lo mostrado por la experiencia nacional, se hace evidente que en materia de *CIBERSEGURIDAD* y *CIBERDEFENSA* estamos recién comenzando, en comparación con países de la Región se hace evidente que estamos en una situación de desventaja en cuanto a la detección y respuesta ante incidente *CIBERNETICO.*

Para un país como Austria, entienden los *CIBERATAQUES* como:

"Attacks from cyber space pose a direct threat to our safety and the proper functioning of the state, economy,

[361] PECERT.COM – Portal del PeCert, http://www.pecert.gob.pe/pecert-acerca-de.html, Información sustraída: 24/04/2016

science and society. They may have a profound negative impact on our daily lives."[362]

"Los ataques de ciberespacio suponen una amenaza directa a nuestra seguridad y el buen funcionamiento del Estado, la economía, la ciencia y la sociedad. Ellos pueden tener un profundo impacto negativo en nuestra vida diaria"[363]

Es necesario entender que efectivizar nuestro mecanismos, será un paso previo para fortalecer los servicios Estatales. Como bien podemos apreciar no se trata de una tendencia aislada de algunos *ESTADOS* es más bien un nuevo modelo del cual todos los *ESTADOS* están sumando esfuerzos para contra restar incidentes negativos.

"Effective digital infrastructures are a prerequisite for providing services of general interest such as energy, water and transport to the population. To allow citizens to realise the benefits promised by our globalised and digitised world, digital infrastructures must function reliably and securely."[364]

"Infraestructuras digitales eficaces son un requisito previo para la prestación de servicios de interés general como la energía, el agua y el transporte a la población. Para permitir que los ciudadanos se dan cuenta los beneficios prometidos por nuestro mundo globalizado y digitalizado, infraestructuras digitales deben funcionar de forma fiable y segura."[365]

---

[362] AUSTRIAN CYBER SECURITY STRATEGY - https://www.bka.gv.at/DocView.axd?CobId=50999, Información sustraída: 24/04/2016
[363] Google traductor.
[364] AUSTRIAN CYBER SECURITY STRATEGY - https://www.bka.gv.at/DocView.axd?CobId=50999, Información sustraída: 24/04/2016
[365] Google traductor

Según el último informe de *CIBERSEGURIDAD* realizado por el *BID* en el 2016:

> "*Según algunos cálculos, el cibercrimen le cuesta al mundo hasta US$575.000 millones al año, lo que representa 0,5% del PIB global. Eso es casi cuatro veces más que el monto anual de las donaciones para el desarrollo internacional. En América Latina y el Caribe, este tipo de delitos nos cuestan alrededor de US$90.000 millones al año. Con esos recursos podríamos cuadruplicar el número de investigadores científicos en nuestra región."*[366]

Si bien, es evidente que las cifras no muestra el monto que afecta a Perú, también es evidente que en un futuro no lejano podría afectar cada vez más a todos los *ESTADOS* incluyendo Perú.

El *BID* a través de su informe nos dice:

> *"La realidad contundente de nuestro tiempo es que el Internet ha revolucionado la forma en que interactuamos con los demás y el mundo que nos rodea. El aumento de la conectividad a Internet hace que un número cada vez mayor de personas estén conectadas en un espacio en gran parte público y transnacional, y proporciona una plataforma dinámica y de crecimiento que permite que avance la comunicación, la colaboración y la innovación en maneras en que nunca hubiéramos podido imaginar hace muy poco tiempo. Esto es particularmente cierto en América Latina y el Caribe, donde más de la mitad de nuestra población ya está en línea y la tasa de crecimiento de usuarios de Internet se encuentra entre las más altas del mundo. En las Américas y el Caribe estamos utilizando el Internet para compartir ideas y cultura; para mejorar el gobierno y los servicios sociales; para colaborar en la*

[366] CIBERSEGURIDAD ¿ESTAMOS PREPARADOS EN AMERICA LATINA Y EL CARIBE?, Informe Ciberseguridad 2016, Pp. 9, Información sustraída: 24/04/2016.

educación, las ciencias y las artes; y para hacer negocios, todo con una mayor accesibilidad y eficiencia. Los mayores beneficios de este nuevo paradigma que está emergiendo rápidamente es el impacto que ha tenido en la estimulación de un nuevo crecimiento y desarrollo social y económico de la región."[367]

Así mismo el informe hace un llamado a los *ESTADOS* para que tomen atención a esta materia, entendiendo que más de la mitad de la población de nuestra región se encuentra conectada a un dispositivo con acceso a *INTERNET.*

"Esto requiere que cultivemos una comprensión de todo el alcance de las amenazas a nuestro dominio cibernético, basado en la más completa y actualizada información disponible. Sin embargo, hay una escasez de literatura integral en materia de seguridad cibernética en América Latina y el Caribe. Desde 2013, el Programa de Seguridad Cibernética del CICTE de la OEA ha tratado de abordar este vacío de información a través de una serie de informes integrales, preparados y publicados en colaboración con líderes de la industria de seguridad cibernética. Estos informes han sido muy explicativos, ofreciendo la imagen más detallada y precisa a la fecha de la seguridad cibernética y la delincuencia cibernética en nuestro hemisferio."[368]

Continúa de la siguiente manera:

"La conectividad a Internet acelera el crecimiento económico y crea oportunidades para los negocios y el comercio. La maximización del valor de la Internet y el ciberespacio debe ser una parte central de la planeación

[367] CIBERSEGURIDAD ¿ESTAMOS PREPARADOS EN AMERICA LATINA Y EL CARIBE?, Informe Ciberseguridad 2016, Pp. 11, Información sustraída: 24/04/2016.
[368] Ob. cit 12, Información sustraída: 24/04/2016.

gubernamental. Sin embargo, estas oportunidades siempre traen sus riesgos. Las tecnologías de Internet aún no están maduras. Los delincuentes las pueden explotar fácilmente. Este riesgo es manejable, pero requiere de la atención de los líderes nacionales. Para que el tema de la seguridad cibernética llegue al nivel más alto del liderazgo político, todavía depende de varios factores: el interés personal, haber experimentado directamente la acción cibernética maliciosa y las relaciones con otros Estados. Sin embargo, un número creciente de presidentes y primeros ministros de todo el mundo han convertido la seguridad cibernética en una prioridad."[369]

La materialización de los intereses vertidos en el informe, podría ser el fortalecimiento de los ordenamientos a través del convenio de *BUDAPEST*, el cual es tomado por el *INFORME,* de la siguiente manera:

"En primer lugar, la región debería continuar su labor en la creación de una base jurídica armonizada para abordar los delitos cibernéticos. El mejor vehículo para esa cooperación es la Convención de Budapest sobre el delito cibernético."[370]

Es necesaria la creación de un ordenamiento jurídico nuevo y vivo que evolución tan rápido como las nuevas tecnologías, un ordenamiento que permita que la realidad cambiante en esta materia no deje al *ESTADO* en una situación de indefensión por el lento movimiento que implicaría adaptarse legislativamente a una nueva forma o tipo de comisión de un *INCIDENTE CIBERNETICO.*

El *BID* continuando con su recomendación, nos dice:

"En segundo lugar, sería útil seguir avanzando para llegar a un entendimiento común sobre las infraestructuras

[369] CIBERSEGURIDAD ¿ESTAMOS PREPARADOS EN AMERICA LATINA Y EL CARIBE?, Informe Ciberseguridad 2016, Pp. 18, Información sustraída: 24/04/2016.
[370] Ob. cit Pp. 19, Información sustraída: 24/04/2016.

críticas y sus vulnerabilidades (una cuestión planteada por el experto colombiano en el GEG[371]), incluyendo una definición compartida de infraestructuras cruciales."[372]

Si, pues las *INFRAESTRUCTURAS CRITICAS* son la parte sensible dentro de las organizaciones *ESTATALES,* y son a través de las cuales los *CIBERCRIMINALES* pueden ejercer un daño mucho mayor a los *ESTADOS.*

El siguiente punto tocado por el *BID*, se encuentra relacionado a la base de toda la *INTERNET*, los *USUARIOS*. Con esta creciente exposición que venimos sufriendo debido a la gran y creciente cantidad de métodos que crean los *CIBERCRIMINALES* para lograr sus objetivos, es necesario, crear mecanismo que generen *CONFIANZA* en el *USUARIO,* esto debido a que son los *USUARIOS* lo consumidores y los que mantienen la *INTERNET*, y ayudan a que esta se desarrolle.

"En tercer lugar, sería beneficioso contar con un enfoque regional más formal para la generación de confianza, a partir de la "Lista Consolidada de Medidas de Fomento de Confianza y Seguridad" y basándose en el trabajo de la OSCE. Esto implicaría el intercambio de documentos nacionales de políticas y leyes, reuniones periódicas entre funcionarios relevantes, incluidos los funcionarios a nivel político, para discutir temas de la estabilidad, comercio y seguridad y el fortalecimiento de redes de cooperación de funcionarios responsables a disposición para consulta inmediata o asistencia en caso de una emergencia."[373]

Y como último punto tocado por el *BID* como propuesta para mejorar la realidad *CIBERNETICA:*

"El contar con una estrategia aporta cierto grado de organización y coherencia a los esfuerzos nacionales y

[371] Grupo de Expertos Gubernamentales.
[372] CIBERSEGURIDAD ¿ESTAMOS PREPARADOS EN AMERICA LATINA Y EL CARIBE?, Informe Ciberseguridad 2016, Pp. 19, Información sustraída: 24/04/2016.
[373] Ob. cit Pp. 19, Información sustraída: 24/04/2016.

ofrece transparencia y seguridad tanto para ciudadanos como para países vecinos. El desarrollo de una estrategia es, por supuesto, una prerrogativa nacional, pero hay muchas ventajas en un enfoque de colaboración para el debate y desarrollo de este tipo de estrategias."[374]

Es necesario entender que con respecto al *CIBERESPACIO, INTERNET, CIBERSEGURIDAD, CIBERDEFENSA*; contar con la colaboración internacional es necesario, debido a que en materia *CIBER* la forma de cometer o perpetrar ilícitos no responde a los límites físicos conocidos, entonces se hace necesario que el Perú establezca alianzas estratégicas con los países de la región y organismos internacionales en materia de *CIBERSEGURIDAD* y *CIBERDEFENSA.*

"Los países necesitan un órgano de coordinación en las oficinas de la Presidencia o del Primer Ministro para supervisar la aplicación, coordinar las gestiones de las entidades y, a veces, resolver disputas. La estrategia debe asignar responsabilidades para la seguridad cibernética entre los ministerios pertinentes y estos ministerios deben desarrollar fuertes lazos con el sector privado para crear un enfoque de colaboración, en particular con la energía eléctrica, las telecomunicaciones y las finanzas. Los gobiernos nacionales necesitan organizaciones de seguridad cibernética adecuadamente atendida que incluyan como mínimo un CERT nacional y policía cibernéticamente capaz."[375]

Como bien mostramos líneas arriba, nuestro *PECERT*, tiene que el ente encargado de monitorear todos aspectos relacionados a los *INCIDENTES CIBERNETICOS*, pero estos esfuerzos no son aislados, es necesario que el *PECERT*, cuente con personal capacitado así como una policía *CIBERNETICA*

[374] Ob. cit Pp. 20, Información sustraída: 24/04/2016.
[375] CIBERSEGURIDAD ¿ESTAMOS PREPARADOS EN AMERICA LATINA Y EL CARIBE?, Informe Ciberseguridad 2016, Pp. 20, Información sustraída: 24/04/2016.

que sea capaz de afrontar el tremendo reto de determinar cuando estamos frente a una *CIBERINCIDENTE,* y con la posibilidad de determinar a sus autores.

Resulta desalentador que ante una amenaza tan grande los *ESTADOS* no destinen fondos para implementar de manera correcta los *CSIRT*[376]*.*

> *"…los gobiernos ignoran la seguridad cibernética, lo cual es muy riesgoso. A medida que todas las sociedades se vuelvan más dependientes de las máquinas y las redes soportadas por computadores (y esto es inevitable ya que las computadoras están incrustadas en los objetos de uso cotidiano, tanto en los automóviles como en maquinaria industrial), la necesidad de adelantar acciones crecerá. En esto, el Hemisferio Occidental ha avanzado mucho, pero aún queda mucho trabajo por hacer."*[377]

El desarrollo de esta materia, como dijimos líneas arriba, no es un esfuerzo aislado, será necesario de esfuerzos conjuntos continuos, en donde el cruce de información sea cada más cotidiano y se mejoren los mecanismo de intercambio de información, ya sea entre entidades públicas o entre éstas y privados o inclusive *USUARIOS,* siendo estos una fuente de información primordial a la cual el *ESTADO* deberá de acudir en todo momento para poder acceder a información para así afrontar de mejor manera algún *INCIDENTE.*

> *"En las regiones desarrolladas del mundo, las estrategias de seguridad cibernética tienen un enfoque integral, que abarca aspectos económicos, sociales, educativos, jurídicos, de aplicación de la ley, técnicos, diplomáticos, militares y relacionados con la inteligencia. Las consideraciones de soberanía en la formulación de políticas de seguridad cibernética son cada vez más*

[376] Equipo de Respuesta a Incidentes de Seguridad de la Información – siglas en ingles
[377] CIBERSEGURIDAD ¿ESTAMOS PREPARADOS EN AMERICA LATINA Y EL CARIBE?, Informe Ciberseguridad 2016, Pp. 20, Información sustraída: 24/04/2016.

relevantes y se puede notar una mayor participación de los militares y de las ramas de inteligencia del gobierno. Sin embargo, cuando las estrategias de seguridad cibernética se centran exclusivamente en asuntos militares y de inteligencia, es posible que no alcancen un equilibrio adecuado entre la seguridad y los derechos, tales como la privacidad y la libertad de expresión y de asociación."[378]

El *BID* reconoce la necesidad de conservar la confianza de los *USUARIOS* en la *INTERNET:*

"…las consecuencias de no protegerla puede afectar la confianza de las actividades en línea, que tiene consecuencias potencialmente negativas para la economía de Internet y en la sociedad en su conjunto."[379]

Es necesario entender a la confianza con fundamental en la *INTERNET,* esta ha sido la base de todo el desarrollo que hasta el momento hemos sido testigos, el desarrollo económico, social, político, etc, se ha venido dando en base a que la confianza en la *INTERNET* viene creciendo, y esto se multiplica por la cantidad de *USUARIOS* que diariamente se conectan a esta *RED.*

El *BID* hace las siguientes recomendaciones:

a. Definir y hacer cumplir los marcos regulatorios de protección de datos y privacidad acertados*.- Es esencial equilibrar la provisión de seguridad con la necesidad de salvaguardar adecuadamente los derechos de los individuos. La aprobación y aplicación de los marcos de privacidad y protección de datos acertados ayudan a lograr este objetivo.*

b. La creación de plataformas nacionales multisectoriales sostenibles*.- Es importante tener en*

[378] Ob. cit Pp. 21, Información sustraída: 24/04/2016.
[379] Ob. cit Pp. 23, Información sustraída: 24/04/2016.

cuenta los diferentes aspectos y consecuencias, así como la viabilidad técnica de la promulgación de nuevas regulaciones. Grupos de la sociedad civil, la academia y la comunidad técnica, así como representantes de la industria pueden proporcionar valiosa experiencia desde sus perspectivas, y ayudar a diseñar un marco reglamentario racional de una manera sostenible. Estas redes de múltiples partes interesadas podrían ayudar a desarrollar un enfoque con visión de futuro para la seguridad cibernética en la región, que tiene en cuenta los avances tecnológicos, como datificación, grandes datos y la Internet de las cosas, y que tiene en cuenta el impacto de estas tecnologías en la seguridad y privacidad.

c. Fortalecimiento de la cooperación internacional.- *La seguridad cibernética se ha ido integrando cada vez más en el plano internacional. Es importante crear canales para una cooperación a varios niveles entre los gobiernos nacionales y las organizaciones internacionales regionales y mundiales que trabajan en el campo. Fortalecer la cooperación regional también puede facilitar la inclusión significativa de los países de la región en las discusiones globales en curso. La naturaleza sin fronteras de Internet aumenta la importancia de la cooperación internacional y la armonización de los marcos legales."*[380]

1. Adecuar nuestro *CSIRT - PECERT*.

El *CERT* es un centro de respuesta ante *INCIDENTES CIBERNETICOS,* tienen que contar con un estándar de calidad internacional, el cual debe ser acorde a las recomendaciones dadas por expertos en la materia, el *BID,* nos conceptualiza a los *CSIRT* de la siguiente manera:

[380] CIBERSEGURIDAD ¿ESTAMOS PREPARADOS EN AMERICA LATINA Y EL CARIBE?, Informe Ciberseguridad 2016, Pp. 24, Información sustraída: 24/04/2016.

> *"Un Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT, por sus siglas en Inglés) se define como un equipo o una entidad dentro de una agencia que proporciona servicios y apoyo a un grupo particular (la comunidad de destino) con el fin de prevenir, manejar y responder a los incidentes de seguridad de la información. Estos equipos están compuestos generalmente por especialistas multidisciplinarios que actúan de acuerdo con los procedimientos y políticas predefinidos para responder rápida y eficazmente a los incidentes de seguridad y para reducir el riesgo de ataques cibernéticos. Hay cientos de CSIRT en el mundo que varían en su misión y alcance. Una de las principales formas de clasificar a los CSIRT es agruparlos por el sector o la comunidad a los que sirven."*[381]

Las recomendaciones hechas por el BID, para la situación en la que se encuentra el Perú son de necesaria atención, y con respecto a nuestro *Equipo de Respuesta ante Incidentes de Seguridad Informática,* es necesario que junto con la implementación que lleva implícito, es necesario que se aplique políticas acorde para que el PeCert no se encuentre solo en una posible situación.

Siguiendo con la experiencia de Austria, ¿QUE ES UNA POLITICA DE CYBER SEGURIDAD?

> *"A comprehensive cyber security policy means that external and internal security as well as civilian and military security aspects are closely interlinked. Cyber security goes beyond the purview of traditional security authorities and comprises instruments of numerous other policy areas.*

[381] CIBERSEGURIDAD ¿ESTAMOS PREPARADOS EN AMERICA LATINA Y EL CARIBE?, Informe Ciberseguridad 2016, Pp. 27, Información sustraída: 24/04/2016.

An integrated cyber security policy must place emphasis on task-sharing between the state, the economy, academia and the civil society. It comprises measures in the following areas: politicalstrategic management, education and training, risk assessment, prevention and preparedness, recognition and response, limitation of effects and restoration as well as the development of governmental and non-governmental capabilities and capacities. An integrated cyber security policy has to be based on a cooperative approach both at national and international level.

A proactive cyber security policy means to work towards preventing threats to cyber space and the people in cyber space or mitigating their impact (configuring security)

A cyber security policy based on solidarity takes account of the fact that – due to the global nature of cyber space – today the cyber security of Austria, the EU and the entire community of nations is interconnected very closely. Intensive cooperation based on solidarity at European and international level is therefore required to ensure cyber security."[382]

"Significa una política integral de seguridad cibernética que la seguridad externa e interna, así como aspectos civiles y militares de seguridad estén estrechamente vinculados entre sí. La seguridad cibernética va más allá de la competencia de las autoridades de seguridad tradicionales y cuenta con numerosos instrumentos de otras áreas de la política.

Una política integral de seguridad cibernética debe poner énfasis en tareas entre el Estado, la economía, la academia y la sociedad civil. Comprende medidas en las siguientes áreas: política estratégica de la gestión, la educación y la

[382] AUSTRIAN CYBER SECURITY STRATEGY, Viena 2013, pp. 6 - https://www.bka.gv.at/DocView.axd?CobId=50999, información sustraída: 30/04/2016.

formación, evaluación de riesgos, prevención y preparación, reconocimiento y respuesta, la limitación de los efectos y la restauración, así como el desarrollo de medios y capacidades gubernamentales y no gubernamentales. Una seguridad informática integrada, la política tiene que basarse en un enfoque de cooperación tanto a nivel nacional como internacional.

Una política de seguridad informática proactiva significa trabajar en la prevención de amenazas para el ciberespacio, y las personas en el ciberespacio o atenuantes de su impacto (configuración de seguridad).

Una política de seguridad informática basada en la solidaridad tiene en cuenta el hecho de que - debido a lo global de la naturaleza del espacio cibernético - hoy en día la seguridad cibernética de Austria, la UE y toda la comunidad de las naciones está interconectada muy de cerca. La cooperación intensiva basada en la solidaridad a nivel europeo y por lo tanto se requiere a nivel internacional para garantizar la seguridad cibernética."[383]

Esta recomendación aunada con un ordenamiento jurídico que sea capaz de afrontar la difícil tarea de mitigar o de reaccionar ante supuesto incidente Cibernéticos haría del Perú un país líder en la región en esta materia, generando un apoyo enorme a la región, y ayudando a países como Argentina y Colombia que cuentan con una realidad mucho más avanzada que la del Perú en cuanto a políticas de Ciber seguridad.

En cuanto al ordenamiento jurídico, Austria una vez más a través de su estrategia nos dice:

"The rule of law: Governance in the area of cyber security has to meet the high standards of the rule of law of the Austrian administration and guarantee compliance with human rights, in particular privacy and data protection as

[383] Google traductor.

well as the freedom of expression and the right to information."[384]

"El estado de derecho: Gobierno en el ámbito de la seguridad informática tiene que cumplir con los altos estándares del estado de derecho de la administración austriaca y garantizar el cumplimiento de los derechos humanos, en particular, la privacidad y protección de datos, así como la libertad de expresión y el derecho a la información."[385]

Si bien, no nos muestra Austria como tiene su ordenamiento jurídico, nos da parámetros mínimos a través de los cuales el Estado debe de guiarse para no salirse de Estado de Derecho[386].

Consideramos que para realizar una propuesta básica y tangible que ayude a mejor posicionarnos con respecto a la Ciber Seguridad y la Ciber Defensa, debemos entender que dentro de la cadena que se crea entre el Estado, las Empresa proveedoras de servicios de internet, las infraestructuras críticas y los usuarios; el eslabón más débil son los usuarios. Entonces la pregunta que debemos plantearnos seria: ¿COMO FORTALECER EL ESLABON MAS DEBIL DENTRO DE LA RED? Para responde la pregunta, utilizaremos la propuesta por la que apuesta España, fortalecer la confianza, pero para ellos es necesario que es la confianza en materia Cibernetica.

Para comenzar utilizaremos lo escrito por el Dr. José Antonio Marina Torres:

"La palabra "conciencia" tiene dos significados. El primero, darse cuenta, percatarse de algo. En nuestro caso, de la importancia, dificultades, complejidades que tiene la seguridad y defensa de una nación, el segundo significado equivale a "conciencia moral", y hace referencia a los

[384] AUSTRIAN CYBER SECURITY STRATEGY, Viena 2013, pp. 6 - https://www.bka.gv.at/DocView.axd?CobId=50999, información sustraída: 30/04/2016.
[385] Google traductor.
[386] Estado de Derecho.- es aquel que se rige por un sistema de leyes e instituciones ordenado en torno de una constitución, la cual es el fundamento jurídico de las autoridades y funcionarios, que se someten a las normas de ésta.

deberes, responsabilidades y al modo de cumplirlos. Una persona dormida, anestesiada o en coma no tiene conciencia en el primer sentido. Un criminal, un psicópata, no tiene conciencia en el segundo. Hago esta reflexión lingüística porque en el caso de la "conciencia de defensa" hay que utilizar ambos significados. Se trata de conocer la importancia, las dificultades, los problemas que plantea, y, también, la responsabilidad persona, ciudadana, ética y política."[387]

Con estas ideas comenzamos el desarrollo de la propuesta *CONCIENCIA* en Ciber seguridad y Ciber Defensa, así nos dice Hidalgo Tarrero:

"También en el caso de la conciencia nacional de ciberseguridad hay que utilizar ambos significados porque es necesario ser conscientes de las amenazas y es necesario conocer nuestros deberes como individuos, como miembros de diversas organizaciones, de la administración y de instituciones y como directivos, en su caso, de ellas; debemos ser conscientes de nuestras responsabilidades tanto individuales como colectivas en el campo de la ciberseguridad; estas responsabilidades son; como en el texto transcrito, personales, ciudadanas, éticas y políticas."[388]

Entonces haciendo que los Usuarios sean conscientes de la realidad y del peligro que se corre en la Internet es suficiente para mejorar los estándares de Ciber seguridad? Pues no, al respecto nos dice Hidalgo:

"La conciencia nacional de ciberseguridad, para que sea nacional, debe incluir a todos los ciudadanos y todas las instituciones, empresas y organización pues de lo contrario presentara carencias y flancos débiles que serán usados, sin ninguna duda, por los atacantes."[389]

---

[387] MARINA TORRES, José Antonio, Cuaderno de Estrategia N° 155, Instituto Español de Estudios Estrategicos, Capitulo Segundo, pp 68.
[388] HIDALGO TARRERO, José Tomás. Monografías 137, Necesidad de una conciencia nacional de CIberseguridad. La Ciberdefensa: un reto prioritario. Pp. 38.
[389] Ob. cit ídem.

Entonces, es necesario que el esfuerzo para fortalecer la conciencia sea ejercido por todos los sujetos que participan o utilizan la internet; o se relacionan a través de ella, si bien hemos dejado en claro que el eslabón débil dentro de la relación que genera la internet son los usuarios, también es clara la idea que no son el único punto de necesaria atención, las vulnerabilidades en materia cibernética o informática nacen de cualquiera de los sujetos esto debido a que dependerá la habilidad del atacantes encaminar una a través de uno y otro medio, bien lo muestra las experiencias que hemos mostrado en capítulos anteriores.

Hidalgo continua reforzando su idea de la siguiente forma:

> *"Si la ciberguerra alcanza a todos los ciudadanos tanto en sus efectos como en sus medios, parece lógico que los ciudadanos, que ya están involucrados voluntaria o involuntariamente, tomen conciencia de ello y participen en la defensa. Pero no solo la ciberguerra alcanza a todos los ciudadanos; también el cibercrimen, que utiliza los mismos medios o parecidos pero con otros fines, tiene como objetivo a cualquier ciudadano. Por esto la conciencia de ciberseguridad debe ser nacional pues de otra manera siempre habrá puertas abiertas para que los atacantes, sean ciberguerreros o cibercriminales, tengan más probabilidades de éxitos al no ofrecer un frente, una muralla solidad y completa."*[390]

Entonces como podríamos empezar a emprender esta ardua tarea de fortalecer algo tan subjetivo de medir como la conciencia, según Hidalgo, podemos establecer los siguientes principios para dar un primer paso:

> *a. Conocimiento de las amenazas y de los riesgos y asumirlos.*
>
> *b. Notificación por los usuarios de los errores cometidos e incidencias sufridas.*
>
> *c. Información por los responsables de seguridad de los sistemas informáticos de los proveedores de servicios de*

[390] Ob. cit ídem.

internet (ISP), de las instituciones y empresas a los usuarios, miembros, empleados y clientes.
d. Formación de todos, cada uno en el nivel que corresponda, en ciberseguridad.
e. Adaptabilidad de usuarios, instituciones y empresas a las circunstancias cambiantes del ciberespacio. "[391]

Ahora procederemos a desarrollar cada uno de ellos para dejar ideas claras sobre lo que se espera de los principios.

a. CONOCIMIENTO DE LAS AMENAZAS Y DE LOS RIESGOS Y ASUMIRLOS.

El presente principio se encuentra relacionado al ejemplo que citamos sobre la actividad humana de volar, en donde tenemos una clara conciencia del peligro porque es captado a través de nuestros sentidos, a comparación del ciberespacio, que es un ambiente en donde nuestros sentidos no pueden captar el peligro, a menos que un cibercriminal publique información de nosotros o que sustraigan dinero de nuestra cuenta de banco, es por ellos que a pesar que es necesario que todos tengamos la idea clara de las amenazas que corremos en la internet.

Al respecto Hidalgo nos dice:

"…todos los usuarios del ciberespacio, los administradores de los sistemas informáticos, las autoridades, los directivos de las empresas, los diseñadores, programadores, etc, deben der plenamente consciente de las amenazas que hay en el ciberespacio y los riesgos inherentes a las mismas; de esta forma, podrán actuar, cada uno en su ámbito, de

[391] HIDALGO TARRERO, José Tomás. Monografías 137, Necesidad de una conciencia nacional de CIberseguridad. La Ciberdefensa: un reto prioritario. Pp. 42.

manera que las posibilidades de éxito de los ataques se reduzcan."[392]

Como bien hemos dicho líneas arriba:

"El tener consciencia de las ciberamenazas no quiere decir que haya que evitar hacer uso del ciberespacio, sino que implica hacer un uso responsable del mismo."[393]

Que significa hacer un uso responsable del ciberespacio? Para responder Hidalgo, nos dice:

"Pere hacer un uso irresponsable del ciberespacio puede llevar que no podamos disponer de energía eléctrica o de otros servicios básicos. No me refiero con uso irresponsable a un uso delictivo, que será perseguido con arreglo al ordenamiento legal vigente, sino simplemente a un uso negligente, posiblemente por desconocimiento, del ciberespacio al no tener correctamente configurado el sistema operativo o no tener antivirus actualizado, por citar un par de ejemplos."[394]

b. <u>NOTIFICACION POR LOS USUARIOS DE LOS ERRORES E INCIDENCIAS SUFRIDAS.</u>

Notificando las incidencias que ocurren o que pasan los usuarios, la internet se alimenta de información de primera mano sobre las nuevas modalidades que utilizan los cibercriminales para perpetrar sus actos, esta es una herramienta que debe utilizarse e implementarse como para que los usuarios tengan la posibilidad de enviar información a las empresas pertinentes para que puede mejor sus sistemas y ofrecer mejoras servicios de seguridad.

"En el ciberespacio los usuarios deberías notificar al responsable de ciberseguridad de su organización, o de su

[392] Ob. cit Pp. 43.
[393] Ob. cit idem
[394] Ob. cit idem.

> ISP si es en el entorno del hogar, todas las incidencias, incluso los errores propios aunque crea que no están directamente relacionados con ataques informáticos."[395]

Según Hidalgo el presente principio es un tanto delicado de afrontar, esto debido a:

> "Significa un cambio de mentalidad, un giro copernicano en la actitud de los ciudadanos. Admitir que hemos cometido un error no es lo habitual, ni siquiera admitirlo en la intimidad; pero es necesario que todos los usuarios colaboren contando a los responsables de seguridad del sistema que utilizan, en el caso de los hogares y las pymes con menos recursos, las incidencias sufridas y los errores cometidos. El responsable de seguridad informática les guiara y dará consejos para evitar los errores. Debemos ser plenamente conscientes de que errar es de humanos y de que al mejor escribano le cae un borrón; todos cometemos errores y son errores porque son fallos no intencionados debidos a falta de conocimiento estrés, etc., y por ello no perdemos ni categoría ni imagen ni nada. Repetir los errores por no reconocerlos y no pedir la ayuda necesaria sí que implica orgullo desmedido y eso no es bueno ni para las personas ni para las organizaciones."[396]

Es debido a lo dicho por Hidalgo que se hace necesario que todos los actores del internet sepamos bien cuál es nuestro rol dentro de esta relación. Es necesario que los usuarios reportemos los incidentes y es necesario que las personas o entidades que recepcionan la información se encuentre debidamente capacitadas para poder orientar a los usuarios para no volver a cometer el mismo error.

[395] Ob. cit ídem.
[396] HIDALGO TARRERO, José Tomás. Monografías 137, Necesidad de una conciencia nacional de CIberseguridad. La Ciberdefensa: un reto prioritario. Pp. 45.

c. INFORMACIÓN POR LOS RESPONSABLES DE SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS DE LOS ISP, DE LAS INSTITUCIONES Y EMPRESAS A LOS USUARIOS, MIEMBROS, EMPLEADOS Y CLIENTES.

Asi como los usuarios debemos de informar y recibir capacitación, la mejor forma de aprender es hacer e conocimiento a los demás usuarios del conocimiento adquirido por parte de estas empresas, es un sistema que permite retroalimentarnos con las experiencias ajenas.

> *"En el ámbito de la seguridad informática, los responsables de seguridad de los sistemas informáticos deberían, al igual que se hace en el ámbito de la seguridad de vuelo, elaborar, cada uno dentro de su ámbito y en colaboración con los homólogos de otras empresas, administraciones, instituciones e ISP, boletines de información sobre ciberseguridad y recibir y analizar las notificaciones de incidencias de los usuarios del sistema del que es responsable. Además, son también responsables de diseñar una política de ciberseguridad, que será aprobada por la dirección o autoridad competente, y de difundirla."*[397]

Una de las formas de difusión de las experiencias obtenidas, sería la siguiente:

> "…las mismas redes que se utilizan en el ciberespacio facilitan la difusión de los boletines de ciberseguridad. En este aspecto siempre es preferible pecar por exceso que por defecto. Los delincuentes suelen preferir objetivos fáciles y poco defendidos que aquellos otros que saben que están bien defendidos y el persona alerta."[398]

Los boletines son medios a los cuales los usuarios podemos tener acceso, pero generar el hábito de hacer es algo que dependerá de cada uno de los

[397] Ob. cit Pp. 47.
[398] HIDALGO TARRERO, José Tomás. Monografías 137, Necesidad de una conciencia nacional de CIberseguridad. La Ciberdefensa: un reto prioritario. Pp. 47.

miembros de la internet. Con el hecho de tener la conciencia de los peligros de los cuales podemos ser víctimas en el ciberespacio, debemos entender que con el conocimiento compartido sobre ciberincidentes podremos afrontar mejor alguna situación.

> *"Los boletines deben estar redactados de forma sencilla y amena porque van dirigidos tanto al personal que tiene una formación sólida en informática y ciberseguridad como a aquellos usuarios que carecen de ella aunque la tengan en otras áreas del conocimiento."*[399]

d. FORMACION DE TODOS, CADA UNO EN EL NIVEL QUE CORRESPONDA EN "CIBERSEGURIDAD"

Como ya hemos mencionado el conocimiento que podemos tener acerca de los incidentes ocurridos nos ayudara a aumentar los índices de seguridad si esto lo aplicamos todo lo actores.

> *"Desde la escuela a la universidad, desde los más jóvenes a los más mayores, en todas las administraciones, instituciones, empresas, a empleados y desempleados, en el hogar.*
> *No se trata de formar hackers, que también lo es – de White hat hackers*[400]*-, sino de que todos los ciudadanos tengan unas mínimas nociones de cómo mantener su entorno cibernético seguro, de que y como se puede publicar en el ciberespacio sin comprometer la privacidad, confidencialidad y disponibilidad de esos datos. Así mismo, hay que enseñar a todos los ciudadanos a utilizar las herramientas básicas de ciberseguridad como pueden ser*

[399] Ob. cit ídem.
[400] White hat hacker es el nombre dado a los hackers que trabajan en empresas y organizaciones, publicas y privadas, para probar los sistemas informáticos que produce y/o usa la empresa u organización para la que trabajan.

antivirus, configuración del firewall y actualizaciones automáticas."[401]

Los que implica la educación en materia cibernética, para poder tener herramientas básicas, abarca nos solo a la educación superior, se hace extensivo desde los primero años de formación hasta después de la formación permanecer en constante capacitación y actualización.

e. ADAPTABILIDAD DE USUARIOS, INSTITUCIONES Y EMPRESAS A LAS CIRCUNSTANCIAS CAMBIANTES DEL CIBERESPACIO.

El ambiente del ciberespacio es una ambiente el cual, en materia de ciberdelincuencia, se desarrolla a cada minuto, lo cual hace necesario que estemos alertas ante nuevas formar de accionar por parte de los ciberdelincuentes.

"Al ser el ciberespacio un concepto no dimensional, sus posibilidades de cambio y la velocidad a la que ocurren esos cambio son muy grandes, casi podríamos decir que ilimitadas. Esto implica la necesidad de adaptarse a todos eso cambios a la misma velocidad, al menos, con la que se producen."[402]

En definitiva este aspecto "no dimensional" hace que lo que ocurre en el ciberespacio sea desenvuelva y se propague mucho más rápido en el mundo real, es por ellos que la capacidad de adaptación es una condición que los actores del ciberespacio debemos desarrollar.

Luego de haber desarrollar de manera breve los principios en que se asienta la conciencia, debemos preguntarnos si solo los principios serán necesario para dar un primer dentro de los que será un ciberespacio más seguro? Al respecto Hidalgo nos dice:

[401] HIDALGO TARRERO, José Tomás. Monografías 137, Necesidad de una conciencia nacional de CIberseguridad. La Ciberdefensa: un reto prioritario. Pp. 47.
[402] Ob. cit Pp. 49.

"Esos cimientos, cual zapata en una edificación, deben ser la conciencia de los diseñadores, arquitectos y programadores del software en hacer software seguro. Nunca se conseguirá un software que sea totalmente seguro pero debe tenderse a ellos.

De poco vale que los usuarios notifiquen, los responsables de seguridad informática informen, este todo el mundo bien formado en ciberseguridad, las empresas, instituciones, administraciones y usuarios sean flexibles y adaptables y que todos asuman las amenazas; si el software es de mala calidad y, por tanto muy susceptible a los ataques informáticos, al final los ciberdelincuentes serían los "señores" del ciberespacio."[403]

Hidalgo nos muestra una vez más que en el ciberespacio se relacionan varios actores, y mientras más actores se relacionen activa y capacitadamente, la ciberseguridad contara con un estándar mucho mejor posicionándonos en una mejor posición en la región.

Otra recomendación la cual ayudaría mucho, es la formación de esta conciencia en todos los niveles y manera inmediata, como nos dice Hidalgo:

"…la formación de esta conciencia debería empezar de manera inmediata y a todos los niveles, empezando en la escuela, terminando en los centro de mayores y pasando por todos los centros educativos públicos y privados y en todas las instituciones y empresas."[404]

Pero para un país como España, como aterriza la ciberseguridad dentro de políticas de Estado?

"Precisamente el tercer objetivo de la mencionada Estrategia de Seguridad Nacional es sobre seguridad

[403] HIDALGO TARRERO, José Tomás. Monografías 137, Necesidad de una conciencia nacional de CIberseguridad. La Ciberdefensa: un reto prioritario. Pp. 50.
[404] Ob. cit Pp. 52.

informática y consiste en "garantiza un uso seguro de las redes y los sistemas de información a través del fortalecimiento de nuestras capacidades de prevención, detección y respuesta d los ciberataques". Dentro de este objetivo, el Gobierno demuestra su conocimiento de la necesidad de una conciencia nacional de ciberseguridad mediante la línea de acción estratégica número 5, que reza: "Implantación de una cultura de ciberseguridad solidad. Se concienciara a los ciudadanos, profesionales y empresas de la importancia de la seguridad de la información y del uso responsable de las nuevas tecnologías y de los servicios de las sociedad del conocimiento"[405]

Entonces la política de Estado de España es la concienciación? Si bien, suena como algo subjetivo el establecimiento de una política de concienciación en materia de ciberseguridad, es un buen punto de partida para posteriormente desarrollar políticas de Estado más concretas, lo que se busca con generar conciencia es crear una base sólida en donde los usuarios sepa cómo actuar cuando se encuentre en el ciberespacio, conociendo también todas las herramientas con las que cuenta en caso de algún incidente.

"Por tanto, ya tenemos una base de partida: el Gobierno de España esta concienciado impulsa la concienciación y todo parece indicar que es una política de Estado"[406]

Al decir que la política de Estado es la concienciación, se está afirmando que el Estado completo se encuentra enfocado en un mismo objetivo, lo cual implica que desde las máximas autoridades hasta los administrados se encuentre comprometidos con la política de Estado.

"El resto de la administración debe alinearse con la estrategia de ciberseguridd que sancione y publique el

[405] Ob. cit Pp. 53.
[406] Ob. cit ídem.

Gobierno. Esta alineación es muy importante por dos razones:

1. *Demostraría a los ciberatacantes que todas las administraciones se toman la ciberseguridad en serio y que están de acuerdo.*

2. *Sería una contribución importantísima y muy necesaria para la concienciación de la sociedad."*[407]

Entonces tenemos que los usuarios y el Estado deberán alinearse para conseguir el objetivo de mejorar la ciberseguridad, pero será esto suficiente?

> *"El siguiente hito es que los directivos de las empresas sean conscientes de la necesidad de que sus empresas sean ciberseguras. Una buena forma de potenciar esto es que la administración exija haber superado inspecciones de ciberseguridad para poder trabajar con las administraciones, fundamentalmente como proveedores…"*[408]

No es difícil entender, a través de la experiencia Española que todos los elementos de participamos dentro del ciberespacio formamos parte de la ciberseguridad, y así lo demuestra España, explicando cómo debe actuar cada uno de los actores.

> *"Para las empresas que se dedican a producir software y sistemas informáticos, a comercializar servicios telemáticos, incluida la venta por internet, o son proveedores de servicios de Internet, esta concienciación de seguridad debe ir mucho más lejos. Tiene una cuota de responsabilidad en la seguridad de los productos y servicios*

[407] Ob. cit Pp. 54.
[408] Ob. cit ídem.

que comercializan y deben extremas las medidas de seguridad"[409]

No es necesario aclara las diferencias marcadas entre Perú y España, a pesar de dos países unidos para un pasado común, actualmente, económicamente, políticamente, geográficamente, geo estratégica y geo políticamente somos diferentes, por eso es de nuestra opinión que no deberíamos copiar el sistema de ciberseguridad y ciberdefensa Español pero si adaptarnos a la idea de que una política de Estado que busque fortalecer las bases del ciberespacio es necesaria, y un buen ejemplo de ellos es la política de concienciación.

"Una estrategia de ciberseguridad a nivel organización debe cumplir ciertos requisitos; los mas comúnmente aceptados son los siguientes:

1. *Debe poderse implantar.*
2. *Debe entenderse.*
3. *Debe hacerse cumplir.*
4. *Debe definir responsabilidades.*
5. *Debe permitir que siga realizándose el trabajo normal.*
6. *Debe ser exhaustiva.*
7. *Debe incluir mecanismos de respuesta.*
8. *Debe tener mecanismos de actualización.*
9. *Debe cumplir la legislación. "*[410]

Así poco a poco se va agarrando forma la ciberseguridad, algo que consideramos necesario comentar, es así como lo recomendó el BID, implementar el PeCert es necesario pero no solo es necesario contar con un PeCert capacitado y actualizado, también es necesario contar con equipos que realicen pruebas en la red de manera constante, probando de diferentes modos las vulnerabilidades que nuestra redes en infraestructuras criticas posean, en el caso de la experiencia Española:

[409] Ob. cit ídem.
[410] Ob. cit ídem.

> *"Un aspecto a menudo olvidado en las estrategias de seguridad son los equipos rojos, del inglés red team. Estos equipos tienen como misión permanente atacar el sistema para descubrir y evaluar las debilidades y proponer medidas para evitar las mismas; dependiendo del tamaño de las organización, el equipo rojo puede ser o no interno a ella. En el caso de las administraciones y empresas públicas, lo recomendable es que los equipos rojos sean internos. Los equipos rojos de la administración central, deben, así mismo, ser los encargados de ejercer su función en los sistemas informáticos de las infraestructuras críticas."*[411]

Si bien España los reconoce como equipos rojos, estos equipos hacen lo que se conoce Hacking Ético[412]. El Hacking Ético, es una forma de mejorar los sistemas informáticos y cibernéticos, a través de pruebas por parte de personas con conocimientos y habilidades especiales para realizar pruebas de seguridad en los sistemas propios.

> *"En efecto, falta el eslabón principal de todo el sistema: las personas. Es necesario formar a las personas en seguridad informática o ciberseguridad. No todo el mundo puede ni debe tener la misma formación. Los usuarios deben estar formados en buenas practicas, algo así como ciberurbanidad o cibereducación."*[413]

Hidalgo precisa la ciberurbanidad de la siguiente forma:

> *"Esta ciberurbanidad o buenas prácticas de seguridad informática debe ser algo que se repita con frecuencia hasta que la sociedad lo tenga interiorizado como tiene*

[411] HIDALGO TARRERO, José Tomás. Monografías 137, Necesidad de una conciencia nacional de CIberseguridad. La Ciberdefensa: un reto prioritario. Pp. 55.

[412] Hacking Ético.- Es una forma de referirse al acto de una persona usar sus conocimientos de informática y seguridad para realizar pruebas en redes y encontrar vulnerabilidades, para luego reportarlas y que tomen medidas, sin hacer daño.

[413] HIDALGO TARRERO, José Tomás. Monografías 137, Necesidad de una conciencia nacional de CIberseguridad. La Ciberdefensa: un reto prioritario. Pp. 59.

interiorizadas normas de buena educación o buenas maneras.

Algunas de estas buenas prácticas podrían ser las siguientes:

1. *Las contraseñas: como deben ser las contraseñas, cuando hay que cambiarlas, como protegerlas.*

2. *Protección contra virus. El antivirus: su importancia, razones para tenerlo activado y actualizado, necesidad de los análisis periódicos, tipos de análisis, etc.*

3. *Beneficios para el usuario y la organización del cumplimiento de las normas de seguridad y las implicaciones de su incumplimiento para el usuario y para la organización.*

4. *El correo electrónico: buenas prácticas en el uso del correo electrónico, en el envió de adjuntos, que hacer si se recibe correo electrónico de direcciones que no son realmente conocidas aunque nos sean familiares, qué hacer con los adjuntos.*

5. *Que está permitido y que prohibido en la organización respecto del uso de internet.*

6. *Copia de seguridad de los datos: aunque la organización disponga de medios para hacer copias de seguridad, hay que concienciar a los usuarios de la importancia de hacer copia local de los datos que utiliza en el día a día.*

7. *En caso de incidente: que hacer, con quien contactar.*

8. *Medidas de prevención ante la ingeniería social: mostrar y analizar ejemplos de correos electrónicos solicitando claves, adjuntando documentos para reuniones, etc.*

9. *Seguridad en el empleo de dispositivos USB: explicar la importancia que estos dispositivos tienen en las organizaciones y casos como el Stuxnet.*

10. *Normas para el envió de información sensible o clasificada: mostrar claramente que medidas de seguridad deben adoptarse para el envió de dicha información.*

11. *Normas básicas de seguridad de los equipos: uso de protectores de pantalla, el bloqueo del PC, etc.*

12. *Instalación de software por parte del usuario: el software instalado por el usuario en los PC puede poner en riesgo la seguridad de nuestras organizaciones; el software debe ser instalado por un administrador.*

13. *Normas básicas de seguridad en los viajes y, en general, fuera del trabajo: tener siempre vigilado el equipo portátil, cuidado con las conversaciones, etc."*[414]

Con estas ideas dadas por Hidalgo se aclara el panorama de lo que buenas prácticas en el ciberespacio es. Ahora bien con respecto a la ciberurbanidad nos dicen lo siguiente:

> *"La ciberurbanidad debe ser una extensión de las buenas maneras, de la buena educación e incluir normas básicas de protección de las información. Debe inculcarse a todos*

[414] HIDALGO TARRERO, José Tomás. Monografías 137, Necesidad de una conciencia nacional de CIberseguridad. La Ciberdefensa: un reto prioritario. Pp. 60.

los niveles y en todos los ambientes. Las buenas maneras se inculcan desde la familia y la escuela, también se inculca la seguridad vial en las escuelas, por tanto las buenas prácticas en ciberseguridad deben ser parte del currículo de los colegios, institutos, universidad y academias militares. No todas las familias pueden en la actualidad colaborar activamente con las instituciones de enseñanza en la educación básica de ciberseguridad, pero estas instituciones si pueden y deberías hacerlo. No solo porque es un problema de seguridad nacional, es que es también un problema de seguridad personal."[415]

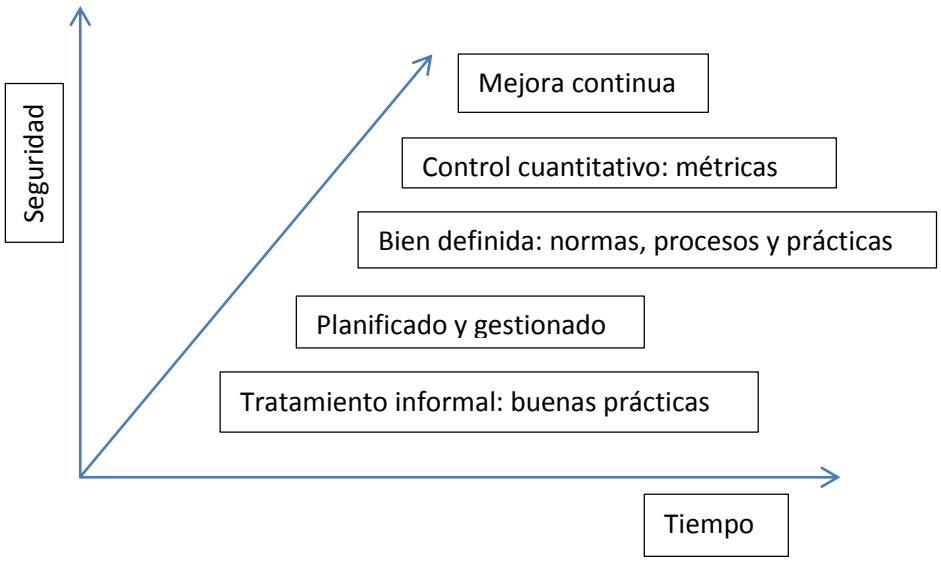

Figura: Niveles de madurez de la implantación de seguridad en una organización (International System Security Engineeing Association)[416]

Con el grafico mostramos la evolución de la ciberseguridad a través de la política establecida por España. Ahora bien, utilizaremos Jiménez Muñoz que nos precisa algunos principios de seguridad:

"En la toma de decisiones en materia de política de seguridad, se deben tener en cuenta una serie de principios

[415] HIDALGO TARRERO, José Tomás. Monografías 137, Necesidad de una conciencia nacional de CIberseguridad. La Ciberdefensa: un reto prioritario. Pp. 60.
[416] JIMÉNES MUÑOZ Luis, Monografías 137, Necesidad de una conciencia nacional de CIberseguridad. La Ciberdefensa: un reto prioritario. Pp. 142.

básicos ampliamente aceptados en el ámbito de la seguridad y que están reflejados en los documentos de política de seguridad de la OTAN y de la Unión Europea así como en los de otro países de nuestro entorno:

1. *Clasificación de la información.*
2. *Habilitación/autorización de seguridad.*
3. *Necesidad de conocer.*
4. *Compartimentación de la información.*
5. *Imputabilidad.*
6. *Equilibrio entre seguridad y eficacia o garantía razonable.*
7. *Segregación de las funciones de administración, administración de seguridad y supervisión de la seguridad."*[417]

Jiménez continúa desarrollando los principios de ciberseguridad:

"Existen además otro principios de seguridad generalmente aceptados y directamente relacionados con los sistemas de información:

1. *Análisis y gestión del riesgo. Se realizaran aquellos procesos necesarios de análisis y gestión de riesgos que permitan monitorizar, reducir, eliminar, evitar o asumir los riesgos asociados al sistema.*

2. *Mínima funcionalidad. Solo estarán disponibles las funciones, protocolos y servicios necesarios para cumplir el requisito operacional o funcional del sistema.*
3. *Mínimo privilegio. Los usuarios de los sistemas que manejen información clasificada solo dispondrán de los privilegios y autorizaciones que se requieren para la realización de las obligaciones de su puesto de trabajo.*

[417] JIMÉNES MUÑOZ Luis, Monografías 137, Necesidad de una conciencia nacional de CIberseguridad. La Ciberdefensa: un reto prioritario. Pp. 150.

4. *Nodo auto protegido. Las medidas de protección deberán implementarse en la medida de lo posible en varios componentes, niveles o capas, y en la máxima extensión, de manera que no haya una única línea (o componente) de defensa.*

5. *Defensa en profundidad. Las medidas de protección deberán implementarse en la medida de lo posible en varios componentes, niveles o capas, y en la máxima extensión, de manera que no haya una única línea (o componente) de defensa.*

6. *Control de configuración. Se debe mantener una configuración básica del equipamiento hardware y software en los sistemas clasificados. Establecer con carácter obligatorio la aplicación de configuración de seguridad en las diferentes tecnologías utilizadas en el sistema.*

7. *Verificación de la seguridad. La aplicación de estos principios y su consecuente implementación en medidas de protección deberá ser inicial y periódicamente verificada.*

8. *Respuesta ante incidentes. Se debe disponer de una capacidad de respuesta que permita una rápida reacción ante un incidente de seguridad."*[418]

España cuenta con un Esquema Nacional de Seguridad, el cual establece los parámetros en materia de seguridad de las tecnologías con respecto al acceso electrónico de los ciudadanos a servicios públicos, y tiene como objetivo:

> *"Su objetivo es establecer la política de seguridad en la utilización de medios electrónicos y está constituido por*

[418] JIMÉNES MUÑOZ Luis, Monografías 137, Necesidad de una conciencia nacional de CIberseguridad. La Ciberdefensa: un reto prioritario. Pp. 150.

principios básicos y requisitos mínimos que permitan una protección adecuada de la información."[419]

Su finalidad es:

"Su finalidad es crear la confianza necesaria en el uso de la administración electrónica por parte de los ciudadanos y permitir el cumplimiento por parte de las administraciones de la obligación de prestar acceso electrónico y tramites públicos"[420]

Sus objetivos principales son:

" 1. Crear las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones Públicas el ejercicios de derecho y el cumplimiento de deberes a través de estos medios.

3. *Establecer la política de seguridad en la utilización de medios electrónicos ene l ámbito de la ley 11/2007, que estará constituida por los principios básicos y los requisitos mínimos para un protección adecuada de la información.*

4. *introducir los elementos comunes que han de guiar la actuación de las Administraciones Publicas en materia de seguridad de las tecnologías de la información.*

5. *Aportar un lenguaje común para facilitar la interacción de la Administraciones Publicas, así como la comunicación de*

[419] Ob. cit Pp. 153.
[420] Ob. cit. idem

los requisitos de seguridad de la información a la industria."[421]

Las recomendaciones realizadas hasta el momento en la presente sección responden a la comparación de las realidades con países como Austria, Colombia y España, así como el último informe en materia de Ciberseguridad para América Latina del 2016.

Consideramos necesario que para implementar un sistema debidamente implementado es necesario conocer las experiencias de países más desarrollados con diferentes posturas en materia de seguridad y defensa para así evaluar de acuerdo a nuestra realidad que es lo que nos conviene de todos los elementos brindados.

[421] JIMÉNES MUÑOZ Luis, Monografías 137, Necesidad de una conciencia nacional de CIberseguridad. La Ciberdefensa: un reto prioritario. Pp. 154.

CONCLUSIONES

1. Hemos encontrado evidencia de la actividad delictiva en las experiencias de países vecinos, con lo cual se hace necesario prestar atención a la materia Cibernética e Informática, debido a que la falta proyección en esta materia podría ocacionar que los Estados sean victima de cada ves mayores y peores incidentes, los cuales pueden ser evitados a traves de un trabajo previo y coordinado, adecuando la tecnología a la nueva realidad en la que el ciber espacio forma parte de la vida cotidiana tanto del Estado como de los ciudadanos.

   Así mismo, hemos encontrado evidencia de ataques cibernéticos al Perú, con lo cual se materializa la situación de vulnerabilidad en la que nos encontramos, si bien hasta donde sabemos, los daños no han sido de gran magnitud, eso no asegura que en un futuro los ataques que el Perú reciba puedan llegar a causar mayor daños.

   Es necesario comentar, que como en el caso ocurrido en Estonia, el ataque puede provenir de un país vecino, el cual posiblemente no tenga intenciones velicas y solo busque realizar espionaje, afectando así a la soberanía Nacional, es por ello que las políticas de Ciberseguridad y Ciberdefensa son de necesaria implementación y ejecución.

2. Una de las mejores medidas para generar conciencia sobre Ciberseguridad es el compartir las experiencias relacionadas a ciberataques con la población, siempre y cuando no se expongan las vulnerabilidades de las entidades o Estados afectados, el límite será siempre establecido al ponderar el derecho de informarnos con la seguridad nacional.

   La evolución de la Ciber Soberanía, no está relacionada a poder ejercer Soberanía sobre el Espacio Cibernético, lo que la evolución de la Soberanía nos muestra es el poder ejercer soberanía sobre las

infraestructura cibernética que se encuentre dentro del territorio de algún Estado. El Estado podrá ejerce las prerrogativas sobre sus Ciber infraestructuras, pudiendo controlar y regular el acceso, desarrollando el pleno ejercicio de defensa de su soberanía, ésta entendida como aquella que debe defenderse a través de las infraestructuras cibernéticas que se encuentran dentro de su territorio.

3. La cibersoberania tendría su campo de acción en la protección de información sensible del estado, pudiendo tener como fuente a infraestructuras críticas o ataques masivos a páginas de servicios públicos que busquen inhabilitarlas. Mientras más conectados a la red nos encontremos, vamos a tener mayor y mejores posibilidades de acceso, vamos a poder enviar y recibir información, realizar operación de manera más rápida y sencilla, pero nos encontraremos más vulnerables frente a hackers o posibles atacantes que busquen filtrarse en nuestros sistemas.

4. La Ciberdefensa tiene como función proteger, detectar, responder y recuperar mientras que la Ciberseguridad serán las medidas para garantizar que los sistemas informaticos y ciberneticos se encuentra protegidos, esto a traves de todo un adamiaje de herramientas que van desde el ordenamiento jurídico hasta las herramientas tecnicas.

5. La realidad creada por internet rompe cualquier limite físico, al afirmar esto es necesario precisar que como la mayoría de actividades humanas, esta también se le puede dar un uso beneficioso como uno maligno, entonces mientras algunas persona utilizan la internet para romper los limites físico y mantener un conversación entre personas que se encuentran una en el polo norte y el otro en el polo sur, habrán personas por otro lado que lo que buscaran en la internet es romper límites físicos para cometer ciberdelitos, pero que el Estado no cuente con una politica adecuada de Ciberseguridad implica dos aspectos, el primero en el cual el Estado debe crear un ordenamiento penal y mecanismo de persecución para los cibercriminales que realizan actividades delicitivas dentro del territorio o que si no son realizadas

dentro tienen como sujeto pasivo al Estado Peruano, y el segundo aspecto es el relacionado a la actividad del Estado como garante de la Ciberseguridad creando un ordenamiento el cual eleve el estándar de seguridad entre el Estado, las empresas prestadoras de servicios ciberneticos e informaticos y los usuarios, es por ellos que de no contar con estas políticas acorde, rompería la estabilidad que el Estado debe propiciar para el correcto desarrollo de la Internet, esto visto desde un punto de vista global en el cual los Estados sean los garantes de ésta.

RECOMENDACIONES

1. A manera de recomendaciones consideramos que el Perú debe de comenzar un proceso de reforma multidisciplinario que tenga como resultado la implementación de políticas, principios, normas, protocolos, directivas en materia de ciberseguridad y ciberdefensa.

2. Destinar los recursos necesarios para implementar un comando de ciberdefensa, que sea capaz de detectar, restaurar, prevenir y contratacar en caso se dé un incidente dentro del territorio nacional, que afecte alguna infraestructura crítica.

3. Implementar y desarrollar "equipos rojos" dentro de las entidades públicas que efectúen hacking ético constante dentro de la red.

4. Establecer estándares a las entidades privadas que suministres software o que sean proveedoras de seguridad, solicitando que cumplan requisitos mínimos de seguridad, esto debido a que forman parte activa de la ciberseguridad.

5. Crear y brindar a los usuarios directivas claras en las cuales tengan la información necesaria en caso de encontrarse en frente de un ciberincidente, el hecho de saber cómo y a quien reportarlo hará que nuestro sistema de ciberseguridad se vea actualizado con información de primer mano para así poder reproducirla y hacer llegar a los usuarios ajenos un reporte el cual sirva para prevenir y educar en materia cibernética e informática.

6. Elaborar panfletos informativos actualizados, escritos de forma sencilla accesible a cualquier persona para que los usuarios puedan recibir una capacitación mínima en la materia y poder reforzar sus niveles de seguridad.

BIBLIOGRAFIA

LIBROS

REMIRO BROTONS, Antonio, Derecho Internacional (I), 1997, pp. 75

OEA – TREND MICRO, Reporte sobre Seguridad Cibernética e Infraestructura Crítica en las Américas, Abril 2015.

SANTIVAÑEZ ANTUNEZ, David Alonso. El delito de terrorismo informático como figura jurídica en el código penal peruano vigente: propuesta para su inclusión en la ley sobre delitos informáticos en el Perú, Tesis para optar el Título de Abogado, Universidad de Lima, 2014.

NARANJO MESA Vladimiro (2014) "Teoría Constitucional e Instituciones Políticas", Colombia, Editorial Temis.

HOBBES, T "Leviatán", I, Madrid, Ed. Sarpe, 1983, Introducción.

LOCKE, Jhon. Ensayos sobre el gobierno civil, Barcelona, Ediciones Orbis, S.A., 1983.

ROUSSEAU, Jean-Jacques. El Contrato Social, Madrid, Ed. Sarpe, 1983.

CHEVALLIER, Jean-Jacques. Los grandes textos políticos, Madrid, Edit. Aguilar, 1981. Pp 153.

SABINE, George H. "Historia de la Teoría Política", Mexico – Bogota, Fondo de Cultura Económica, 1976.

OEA – Tendencia de seguridad cibernética en américa latina y el caribe.

CARRE DE MALBERG, René, Teoría general del Estado, Mexico, Fondo de Cultura Económica, 1948.

TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE. Cambridge University Press.

ROUSSEAU, Charles, Derecho Internacional Público, Barcelona, Edic. Ariel, 1957.

SCHMITT, Carl. Der Begriff des Politischen (El concepto de los políticos). Berlin: s.n., 1932.

HIDALGO TARRERO, José Tomás. Monografías 137, Necesidad de una conciencia nacional de CIberseguridad. La Ciberdefensa: un reto prioritario.

CABRERIZO CALATRAVA, Antonio Jesús. El conflicto asimétrico. Universidad de Granada: I Congreso Nacional de Estudios de Seguridad, 2002.

LIANG, Qiao y XIANGSUI, Wang. Unrestricted Warfare (Guerra sin restricciones). Beijing: PLA Literature and Arts Publishing House, febrero de 1999.

SUN TZU, El Arte de la Guerra, Capítulo I pp.3

TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE. Cambridge University Press, pp. 18.

MARINA TORRES, José Antonio, Cuaderno de Estrategia N° 155, Instituto Español de Estudios Estrategicos, Capitulo Segundo.

HIDALGO TARRERO, José Tomás. Monografías 137, Necesidad de una conciencia nacional de CIberseguridad. La Ciberdefensa: un reto prioritario.

JIMÉNES MUÑOZ Luis, Monografías 137, Necesidad de una conciencia nacional de CIberseguridad. La Ciberdefensa: un reto prioritario. Pp. 142.

CIBERSEGURIDAD ¿ESTAMOS PREPARADOS EN AMERICA LATINA Y EL CARIBE?, Informe Ciberseguridad 2016, Pp. 9.

VILLAVICENCIO TERREROS, Felipe – Delitos informáticos en la Ley 30096 y la modificación de la Ley 30071, pp. 3

NORMAS LEGALES

Tribunal Constitucional Perú - Expediente N.º 05761-2009-PHC/TC, fundamento 29.

Convención Panamericana sobre los Derecho y Deberes de los Estados 1933.

Declaracion de los Derecho del Hombre y del Ciudadano, art. 3 - http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/espagnol/es_ddhc.pdf.

Constitución Política del Perú.

CONVENIO DE BUDAPEST, Convenio sobre Ciberdelincuencia, Articulo I.

CONVENIO DE BERNA PARA LA PROTECCIÓN DE LAS OBRAS LITERARIAS Y ARTISTICAS.

El Tratado de la OMPI sobre Derecho de Autor (WCT) es un arreglo particular adoptado en virtud del Convenio de Berna que trata de la protección de las obras y los derechos de sus autores en el entorno digital. Además de los derechos reconocidos en el Convenio de Berna, se conceden determinados derechos económicos. El Tratado también se ocupa de dos objetos de protección por derecho de autor: i) los programas de computadora, con independencia de su modo o forma de expresión, y ii) las compilaciones de

datos u otros materiales ("bases de datos"). – Información sustraída de: http://www.wipo.int/treaties/es/ip/wct/.

LIBRO BLANCO DE LA DEFENSA DEL PERÚ (2005) Capitulo II pp.45

LIBRO BLANCO DE LA DEFENSA DEL PERÚ (2005) Capitulo II pp.48

Constitución Política del Perú (1993) Titulo II Capítulo I Art. 44.

Libro Blanco de la Defensa Nacional (2005) Presentación del Libro Blanco de la Defensa Nacional.

Constitución Política del Perú, articulo 2, inciso 6.

AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS PERSONALES, Ministerio de Justicia, Guía de Inscripción de Bancos de Datos Personales.

LEY DE PROTECCIÓN DE DATOS PERSONALES, LEY N°29733, art. 2 numeral 4.

CONVENIO DE BUDAPEST, Convenio sobre Ciberdelincuencia.

REVITAS

LA GACETA, "Allanan la casa de un tucumano investigado por "Ciberterrorismo" contra el Ejército de Colombia" Publicado el 20 de Febrero de 2012. En: http://www.lagaceta.com.ar/nota/478615/allanan-casa-tucumano-investigado-ciberterrorismo-contra-ejercito-colombia.html.

elEconomista.es: Telecomunicaciones y Tecnología. "China lanza un Ciberataque contra una teleco australiana por error". Publicado el 15 de abril de 2010. En: http://¿eciduario.eleconomista.es/telecomunicaciones-tecnologia/noticias/2061591/04/10/China-lanza-un-ciberataque-contra-una-teleco-australiana-por-error.html.

Business Week.- Es una revista semanal de negocios publicada por Bloomberg L.P.

REALINSTITUTOELCANO.ORG, Portal de el Cano - http://www.blog.rielcano.org/la-ciber-soberania-china/.

PAGINAS WEB

NATO.INT - Portal de la OTAN - http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm - sitio visitado 25/02/2016.

OTAN, Organización del Tratado del Atlántico Norte, alianza militar intergubernamental.http://www.natolibguides.info/cybersecurity.

FBI.GOV – Portal del FBI, https://www.fbi.gov/about-us/investigate/cyber/law-enforcement-cyber-incident-reporting

Fedrico. Reportaje perteneciente al Programa Televisivo "Informe Central" conducido por Rolando Graña (24/01/2007) "Ciberterrorismo, ¿Mito o Realidad?. En: http://www.youtube.com/watch?v=h4a_QIwbRjE.

JOYE, Christopher. The Australian Financial Review. "Cyber-Attacks penétrate Reserve Bank networks". Publicado el 11 de marzo de 2013. En: http://www.afr.com/p/national/cyber_attacks_penetrate_reserve"FEdCLOl50owRMgl0urEYnK.

OPERACIÓN CONTRA EL CIBERTERRORISMO. "terroristas Informáticos "Antifascistas" publican datos de clientes de comercios sevillanos para ser objetos de sus acciones". Publicado el 28 de Febrero de 2012. En: http://terroristasnogracias.blogspot.com/2012/02/operacion-contra-el-cibercrimen.html Información sustraída: 03/03/2016

RPP.COM.PE – Portal digital de RPP "Recuerde los ataques informáticos más importantes de Anonymous". Publicado 19 de Enero de 2012. En: http://rpp.pe/tecnologia/mas-tecnologia/recuerde-los-ataques-informaticos-mas-importantes-de-anonymous-noticia-442572.

LEB.FBI.GOV – Portal del FBI "CYBER TERROR" - https://leb.fbi.gov/2011/november/cyber-terror.

TREND MICRO, Empresa dedicada al desarrollo de software de Ciber seguridad a nivel mundial, actualmente consultora de CiberSeguridad de la OEA.

TRENDMICRO.COM- Portal de Trend Micro**,** SCADA threats: a new front in the war against cyber crime? - http://blog.trendmicro.com/scada-threats-a-new-front-in-the-war-against-cyber-crime/.

TRENDMICRO.COM- Portal de Trend Micro, SCADA threats: a new front in the war against cyber crime? - http://blog.trendmicro.com/scada-threats-a-new-front-in-the-war-against-cyber-crime/.

TRENDMICRO.COM- Portal de Trend Micro**,** GLOSARIO - http://www.trendmicro.com/vinfo/us/security/definition/apt-advanced-persistent-threat , Publicación sustraída fecha: 13/03/16

TRENDMICRO.COM- Portal de Trend Micro**,** Cloud Security and APT defense – Identical Twins?: http://blog.trendmicro.com/cloud-security-and-apt-defense-identical-twins/.

TRENDMICRO.COM- Portal de Trend Micro**,** Hybrid Cloud: Going Beyond Security in a Software Defined Datacenter: http://blog.trendmicro.com/hybrid-cloud-going-beyond-security-software-defined-datacenter/.

NATO.INT – Portal de la OTAN, INTELLIGENCE EXPLOITATION OF THE INTERNET - http://nsarchive.gwu.edu/NSAEBB/NSAEBB436/docs/EBB-005.pdf.

TRENDMICRO.COM-Portal de Trend Micro, BELOW THE SURFACE: EXPLORING THE DEEP WEB - https://www.trendmicro.com/cloud-content/us/pdfs/securityintelligence/whitepapers/wp_below_the_surface.pdf.

TREND MICRO.COM – Portal de Trend Micro, Deep Web and Cybercrime: It's Not All About Tor - http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/deep-web-and-cybercrime-its-not-all-about-tor.

NATO.INT – Portal de la OTAN, Centro de Excelencia de la OTAN- https://ccdcoe.org/cyber-definitions.html.

NATO.INT – Portal de la OTAN, http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm, Información sustraída: 25/02/2016.

NATO.INT – Portal de la OTAN, ehttp://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm, Información sustraída: 25/02/2016.

ELCOMERCIO.COM.PE – Portal digital de elcomercio "Anonymous atacó varios sitios web del Estado Peruano". Publicado 09 de Setiembre de 2011. En: http://elcomercio.pe/tecnologia/actualidad/anonymous-ataco-hoy-varios-sitios-web-estado-peruano-noticia-1284976.

Peru21.pe – Portal digital del Diario Peru21. "Anonymous filtra 1000 documentos del gobierno peruano". Publicado el 07 de febrero de 2012. En: http://peru21.pe/2012/02/07/actualidad/anonymous-filtra-mil-documentos-gobierno-peruano-2010892.

LAPRENSA.PERU.COM - "Reniec niega hackeo de su base de datos, pero Anonymous ratifica ataque". Publicado el 13 de Marzo de 2015. En: http://laprensa.peru.com/actualidad/noticia-anoymous-peru-base-datos-reniec-niega-hacker-violacion-seguridad-40750.

INEI.GOB.PE – Portal del Instituto Nacional de Estadística e Informática, https://www.inei.gob.pe/estadisticas/indice-tematico/poblacion-y-vivienda/.

LELIVREBLANCDELADEFENSEETSECURITE.GOUV.FR – Portal del Libro Blanco de Defensa y la Seguridad, http://www.livreblancdefenseetsecurite.gouv.fr/pdf/le_livre_blanc_de_la_defense_2013.pdf.

AUSTRIAN CYBER SECURITY STRATEGY, Viena 2013, pp. 6 - https://www.bka.gv.at/DocView.axd?CobId=50999.

NATO.INT - Portal de la OTAN - https://ccdcoe.org/cyber-definitions.html.

RAE.ES

MINDEF.GOB.AR – Portal del Ministerio de Defensa de Argentina, Libro Blanco de la Defensa, http://www.mindef.gov.ar/index.php.

LELIVREBLANCDELADEFENSEETSECURITE.GOUV.FR – Portal del Libro Blanco de Defensa y la Seguridad, http://www.livreblancdefenseetsecurite.gouv.fr/pdf/le_livre_blanc_de_la_defense_2013.pdf.

MINISTERIO DE DEFENSA ARGENTINA – Portal de Ministerio de Defensa de Argentina, http://www.mindef.gov.ar/plantillaNoticia.php?notId=33.

PECERT.COM – Portal del PeCert, http://www.pecert.gob.pe/pecert-acerca-de.html.

AUSTRIAN CYBER SECURITY STRATEGY - https://www.bka.gv.at/DocView.axd?CobId=50999.

RPP.COM.PE – Portal digital de RPP "Recuerde los ataques informáticos más importantes de Anonymous". Publicado 19 de Enero de 2012. En: http://rpp.pe/tecnologia/mas-tecnologia/recuerde-los-ataques-informaticos-mas-importantes-de-anonymous-noticia-442572. Información sustraída: 03/03/2016

LELIVREBLANCDELADEFENSEETSECURITE.GOUV.FR – Portal del Libro Blanco de Defensa y la Seguridad, http://www.livreblancdefenseetsecurite.gouv.fr/pdf/le_livre_blanc_de_la_defense_2013.pdf.

CAPITAL.PE – Portal digital de Radio Capital. "Anonymous Perú hackea web de entidades estatales". Publicado el 28 de Julio de 2013. En: http://www.capital.com.pe/2013-07-28-anonymous-peru-hackea-web-de-entidades-estatales-noticia_617378.html

ELCOMERCIO.COM.PE – Portal digital de el Comercio "Twitter: Anonymous Perú hackeó web de la Municipalidad de Lima" Publicado el 06 de Marzo de 2015. En: http://elcomercio.pe/redes-sociales/twitter/twitter-anonymous-peru-hackeo-web-municipalidad-lima-noticia-1795706?ref=flujo_tags_223948&ft=nota_13&e=titulo.

INI, Fedrico. Reportaje perteneciente al Programa Televisivo "Informe Central" conducido por Rolando Graña (24/01/2007) "Ciberterrorismo, ¿Mito o Realidad?. En: http://www.youtube.com/watch?v=h4a_QIwbRjE.

APENDICE

PROYECTO DE LEY

La presente investigación pretender concluir realizando un aporte jurídico al ordenamiento nacional, con lo cual se pueda continuar con los esfuerzos realizados hasta el momento por el Estado Peruano.

Capítulo I – Terminología

Artículo 1 – Definiciones

A los efectos del presente Convenio, la expresión:

a."sistema informático" designa todo dispositivo aislado o conjunto de dispositivos interconectados o unidos, que aseguran, en ejecución de un programa, el tratamiento automatizado de datos;

b."datos informáticos" designa toda representación de hechos, informaciones o conceptos expresados bajo una forma que se preste a tratamiento informático, incluido un programa destinado a hacer que un sistema informático ejecute una función;

c."prestador de servicio" designa:

i.toda entidad pública o privada que ofrece a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático;

ii. cualquier otra entidad que trate o almacene datos informáticos para ese servicio de comunicación o sus usuarios;

d."datos de tráfico" designa todos los datos que tienen relación con una comunicación por medio de un sistema informático, producidos por este último, en cuanto elemento de la cadena de comunicación, indicando el origen, el destino, el itinerario, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

Capítulo II – Medidas que deben ser adoptadas a nivel nacional

Sección 1 – Derecho penal material

Título 1 – Infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

Artículo 2 – Acceso ilícito

Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, el acceso doloso y sin autorización a todo o parte de un sistema informático. Las Partes podrán exigir que la infracción sea cometida con vulneración de medidas de seguridad, con la intención de obtener los datos informáticos o con otra intención delictiva, o también podrán requerir que la infracción se perpetre en un sistema informático conectado a otro sistema informático.

Artículo 3 – Interceptación ilícita

Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la interceptación, dolosa y sin autorización, cometida a través de medios técnicos, de datos informáticos – en transmisiones no públicas– en el destino, origen o en el interior de un sistema informático, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporta tales datos informáticos. Las Partes podrán exigir que la infracción sea cometida con alguna intención delictiva o también podrán requerir que la infracción se perpetre en un sistema informático conectado a otro sistema informático.

Artículo 4 – Atentados contra la integridad de los datos

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la conducta de dañar, borrar, deteriorar, alterar o suprimir dolosamente y sin autorización los datos informáticos.

2. Las Partes podrán reservarse el derecho a exigir que el comportamiento descrito en el párrafo primero ocasione daños que puedan calificarse de graves.

Artículo 5 – Atentados contra la integridad del sistema

Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la obstaculización grave, cometida de forma dolosa y sin autorización, del funcionamiento de un sistema informático, mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.

Artículo 6 – Abuso de equipos e instrumentos técnicos

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal,

conforme a su derecho interno, las siguientes conductas cuando éstas sean cometidas dolosamente y sin autorización:

a. la producción, venta, obtención para su utilización, importación, difusión u otras formas de puesta a disposición:

i.de un dispositivo, incluido un programa informático, principalmente concebido o adaptado para permitir la comisión de una de las infracciones establecidas en los artículos 2 a 5 arriba citados;

ii.de una palabra de paso (contraseña), de un código de acceso o de datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con la intención de utilizarlos como medio para cometer alguna de las infracciones previstas en los artículos 2 a 5; y

b. la posesión de alguno de los elementos descritos en los parágrafos (a) (1) o (2) con la intención de utilizarlos como medio para cometer alguna de las infracciones previstas en los artículos 2-5. Los Estados podrán exigir en su derecho interno que concurra un determinado número de elementos para que nazca responsabilidad penal.

2. Lo dispuesto en el presente artículo no generará responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, difusión u otras formas de puesta a disposición mencionadas en el párrafo 1 no persigan la comisión de una infracción prevista en los artículos 2 a 5 del presente Convenio, como en el caso de ensayos autorizados o de la protección de un sistema informático.

3. Las Partes podrán reservarse el derecho de no aplicar el párrafo 1, a condición de que dicha reserva no recaiga sobre la venta, distribución o cualesquiera otras formas de puesta a disposición de los elementos mencionados en el parágrafo 1 (a)(2).

Título 2 – Infracciones informáticas

Artículo 7 – Falsedad informática

Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la introducción, alteración, borrado o supresión dolosa y sin autorización de datos informáticos, generando datos no auténticos, con la intención de que sean percibidos o utilizados a efectos legales como auténticos, con independencia de que sean directamente legibles e inteligibles. Las Partes podrán reservarse el derecho a

exigir la concurrencia de un ánimo fraudulento o de cualquier otro ánimo similar para que nazca responsabilidad penal.

Artículo 8 – Estafa informática

Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la producción de un perjuicio patrimonial a otro, de forma dolosa y sin autorización, a través de:

a.la introducción, alteración, borrado o supresión de datos informáticos,

b.cualquier forma de atentado al funcionamiento de un sistema informático, con la intención, fraudulenta o delictiva, de obtener sin autorización un beneficio económico para sí mismo o para tercero.

Título 3 – Infracciones relativas al contenido

Artículo 9 – Infracciones relativas a la pornografía infantil

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, las siguientes conductas cuando éstas sean cometidas dolosamente y sin autorización:

a.la producción de pornografía infantil con la intención de difundirla a través de un sistema informático;

b.el ofrecimiento o la puesta a disposición de pornografía infantil a través de un sistema informático;

c.la difusión o la transmisión de pornografía infantil a través de un sistema informático;

d. el hecho de procurarse o de procurar a otro pornografía infantil a través de un sistema informático;

e. la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos.

2. A los efectos del párrafo 1 arriba descrito, la «pornografía infantil» comprende cualquier material pornográfico que represente de manera visual:

a. un menor adoptando un comportamiento sexualmente explícito;

b. una persona que aparece como un menor adoptando un comportamiento sexualmente explícito;

c.unas imágenes realistas que representen un menor adoptando un comportamiento sexualmente explícito.

3. A los efectos del párrafo 2 arriba descrito, el término «menor» designa cualquier persona menor de 18 años. Las Partes podrán exigir un límite de edad inferior, que debe ser como mínimo de 16 años.

4. Los Estados podrán reservarse el derecho de no aplicar, en todo o en parte, los párrafos 1 (d) y 1 (e) y 2 (b) y 2 (c).

Título 4 – Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines

Artículo 10 – Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, los atentados a la propiedad intelectual definida por la legislación de cada Estado, conforme a las obligaciones que haya asumido por aplicación de la Convención Universal sobre los Derechos de Autor, revisada en París el 24 de julio de 1971, del Convenio de Berna para la protección de obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Derecho de Autor, a excepción de cualquier derecho moral conferido por dichas Convenciones, cuando tales actos sean cometidos deliberadamente, a escala comercial y a través de un sistema informático.

2. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, los atentados a los derechos afines definidos por la legislación de cada Estado, conforme a las obligaciones que haya asumido por aplicación de la Convención Internacional sobre la Protección de los Artistas Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión, hecha en Roma (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre interpretación o ejecución y fonogramas, a excepción de cualquier derecho moral conferido por dichas Convenciones, cuando tales actos sean cometidos deliberadamente, a escala comercial y a través de un sistema informático.

3. Las Partes podrán, de concurrir determinadas circunstancias, reservarse el derecho de no imponer responsabilidad penal en aplicación de los párrafos 1 y 2 del presente artículo, siempre que se disponga de otros recursos eficaces para su represión y que dicha reserva no comporte infracción de las obligaciones

internacionales que incumban al Estado por aplicación de los instrumentos internacionales mencionados en los párrafos 1 y 2 del presente artículo.

Título 5 – Otras formas de responsabilidad y sanción

Artículo 11 – Tentativa y complicidad

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, cualquier acto de complicidad que sea cometido dolosamente y con la intención de favorecer la perpetración de alguna de las infracciones establecidas en los artículos 2 a 10 del presente Convenio.

2. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la tentativa dolosa de cometer una de las infracciones establecidas en los artículos 3 a 5, 7, 8, 9 (1) a y 9 (1) c del presente Convenio.

3. Las Partes podrán reservarse el derecho de no aplicar, en todo o en parte, el párrafo 2 del presente artículo.

Artículo 12 – Responsabilidad de las personas jurídicas

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para permitir que las personas jurídicas puedan ser tenidas por responsables de las infracciones establecidas en el presente Convenio, cuando éstas sean cometidas por una persona física, actuando ya sea a título individual, ya sea como miembro de un órgano de la persona jurídica, que ejerce un poder de dirección en su seno, cuyo origen se encuentre en:

a. un poder de representación de la persona jurídica;

b. una autorización para tomar decisiones en nombre de la persona jurídica;

c. una autorización para ejercer control en el seno de la persona jurídica.

2. Fuera de los casos previstos en el párrafo 1, las Partes adoptarán las medidas necesarias para asegurar que una persona jurídica puede ser tenida por responsable cuando la ausencia de vigilancia o de control por parte de cualquier persona física mencionada en el párrafo 1 haya permitido la comisión de las infracciones descritas en el párrafo 1 a través de una persona física que actúa bajo autorización de la persona jurídica.

3. La responsabilidad de la persona jurídica podrá resolverse en sede penal, civil o administrativa, dependiendo de los principios jurídicos propios del Estado.

4. Esta responsabilidad se establecerá sin perjuicio de la responsabilidad penal de las personas físicas que hayan cometido la infracción.

Artículo 13 – Sanciones y medidas

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para permitir que las infracciones penales establecidas en los artículos 2 a 11 sean castigadas con sanciones efectivas, proporcionadas y disuasorias, incluidas las penas privativas de libertad.

2. Las Partes velarán para que las personas jurídicas que hayan sido declaradas responsables según lo dispuesto en el artículo 12 sean objeto de sanciones o medidas penales o no penales efectivas, proporcionadas y disuasorias, incluidas las sanciones pecuniarias.

Sección 2 – Derecho procesal

Título 1 – Disposiciones comunes

Artículo 14 – Ámbito de aplicación de las medidas de derecho procesal

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para instaurar los poderes y procedimientos previstos en la presente sección a los efectos de investigación o de procedimientos penales específicos.

2. Salvo disposición en contrario, prevista en el artículo 21, las Partes podrán aplicar los poderes y procedimientos mencionados en el párrafo 1:

a. a las infracciones penales establecidas en los artículos 2 a 11 del presente Convenio;

b. a cualquier otra infracción penal cometida a través de un sistema informático; y

c. a la recogida de pruebas electrónicas de cualquier infracción penal.

3. a.Las Partes podrán reservarse el derecho de aplicar la medida mencionada en el artículo 20 a las infracciones especificadas en sus reservas, siempre que el número de dichas infracciones no supere el de aquellas a las que se aplica la medida mencionada en el artículo 21. Las Partes tratarán de limitar tal reserva de modo que se permita la aplicación lo más amplia posible de la medida mencionada en el artículo 20.

b.Cuando un Estado, en razón de las restricciones impuestas por su legislación vigente en el momento de la adopción del presente Convenio, no esté en condiciones de aplicar las medidas descritas en los artículos 20 y 21 a las comunicaciones transmitidas en un sistema informático de un prestador de servicios que

i.es utilizado en beneficio de un grupo de usuarios cerrado, y

ii.no emplea las redes públicas de telecomunicación y no está conectado a otro sistema informático, público o privado, ese Estado podrá reservarse el derecho de no aplicar dichas medidas a tales comunicaciones. Los Estados tratarán de limitar tal reserva de modo que se permita la aplicación lo más amplia posible de las medidas mencionadas en los artículos 20 y 21.

Artículo 15 – Condiciones y garantías

1. Las Partes velarán para que la instauración, puesta en funcionamiento y aplicación de los poderes y procedimientos previstos en la presente sección se sometan a las condiciones y garantías dispuestas en su derecho interno, que debe asegurar una protección adecuada de los derechos del hombre y de las libertades y, en particular, de los derechos derivados de las obligaciones que haya asumido en aplicación del Convenio para la protección de los derechos humanos y libertades fundamentales del Consejo de Europa (1950) y del Pacto internacional de derechos civiles y políticos de Naciones Unidas (1966) o de otros instrumentos internacionales relativos a los derechos del hombre, y que debe integrar el principio de proporcionalidad.

2. Cuando ello sea posible, en atención a la naturaleza del poder o del procedimiento de que se trate, dichas condiciones y garantías incluirán, entre otras, la supervisión judicial u otras formas de supervisión independiente, la motivación justificante de la aplicación, la limitación del ámbito de aplicación y la duración del poder o del procedimiento en cuestión.

3. Las Partes examinarán la repercusión de los poderes y procedimientos de esta Sección sobre los derechos, responsabilidades e intereses legítimos de terceros, como exigencia dimanante del interés público y, en particular, de una correcta administración de justicia.

Título 2 – Conservación inmediata de datos informáticos almacenados

Artículo 16 – Conservación inmediata de datos informáticos almacenados

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para permitir a sus autoridades competentes ordenar o imponer de otro modo la conservación inmediata de datos electrónicos especificados, incluidos los datos de tráfico, almacenados a través de un sistema informático, especialmente cuando hayan razones para pensar que son particularmente susceptibles de pérdida o de modificación.

2. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para obligar a una persona a conservar y proteger la integridad de los datos – que se encuentran en su poder o bajo su control y respecto de los cuales exista un mandato previo de conservación en aplicación del párrafo precedente – durante el tiempo necesario, hasta un máximo de 90 días, para permitir a las autoridades competentes obtener su comunicación. Los Estados podrán prever que dicho mandato sea renovado posteriormente.

3. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para obligar al responsable de los datos o a otra persona encargada de conservarlos a mantener en secreto la puesta en ejecución de dichos procedimientos durante el tiempo previsto por su derecho interno.

4. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.

Artículo 17 – Conservación y divulgación inmediata de los datos de tráfico

1. A fin de asegurar la conservación de los datos de tráfico, en aplicación del artículo 16, las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para:

a. procurar la conservación inmediata de los datos de tráfico, cuando uno o más prestadores de servicio hayan participado en la transmisión de dicha comunicación; y

b. asegurar la comunicación inmediata a la autoridad competente del Estado, o a una persona designada por dicha autoridad, de datos de tráfico suficientes para permitir la identificación de los prestadores de servicio y de la vía por la que la comunicación se ha transmitido.

2. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.

Título 3 – Mandato de comunicación

Artículo 18 – Mandato de comunicación

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para ordenar:

a. a una persona presente en su territorio que comunique los datos informáticos especificados, en posesión o bajo el control de dicha persona, y almacenados en un sistema informático o en un soporte de almacenaje informático; y

b. a un prestador de servicios que ofrezca sus prestaciones en el territorio del Estado firmante, que comunique los datos en su poder o bajo su control relativos a los abonados y que conciernan a tales servicios;

2. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.

3. A los efectos del presente artículo, la expresión «datos relativos a los abonados» designa cualquier información, expresada en datos informáticos o de cualquier otro modo, poseída por un prestador de servicio y que se refiere a los abonados de sus servicios, así como a los datos de tráfico o relativos al contenido, y que permite establecer:

a. el tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el tiempo del servicio;

b. la identidad, la dirección postal o geográfica y el número de teléfono del abonado o cualquier otro número de acceso, los datos relativos a la facturación y el pago, disponibles por razón de un contrato o de un alquiler de servicio;

c. cualquier otra información relativa al lugar donde se ubican los equipos de comunicación, disponible por razón de un contrato o de un alquiler de servicio.

Título 4 – Registro y decomiso de datos informáticos almacenados

Artículo 19 – Registro y decomiso de datos informáticos almacenados

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para registrar o acceder de un modo similar:

a. a un sistema informático o a una parte del mismo, así como a los datos informáticos que están almacenados; y

b. a un soporte de almacenamiento que permita contener datos informáticos en su territorio.

2. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para procurar que, cuando sus autoridades registren o accedan de un modo similar a un sistema informático específico o a una parte del mismo, conforme al párrafo 1 (a), y tengan motivos para creer que los datos buscados se hallan almacenados en otro sistema informático o en una parte del mismo situado en su territorio, y que dichos datos son igualmente accesibles a partir del sistema inicial o están disponibles a través de ese primer sistema, dichas autoridades estén en condiciones de ampliar inmediatamente el registro o el acceso y extenderlo al otro sistema.

3. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para decomisar u obtener de un modo similar los datos informáticos cuyo acceso haya sido realizado en aplicación de los párrafos 1 o 2. Estas medidas incluyen las prerrogativas siguientes:

a. decomisar u obtener de un modo similar un sistema informático o una parte del mismo o un soporte de almacenaje informático;

b. realizar y conservar una copia de esos datos informáticos;

c. preservar la integridad de los datos informáticos almacenados pertinentes; y

d. hacer inaccesibles o retirar los datos informáticos del sistema informático consultado.

4. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para ordenar a cualquier persona, que conozca el funcionamiento de un sistema informático o las medidas aplicadas para proteger los datos informáticos que contiene, que proporcione todas las informaciones razonablemente necesarias,

para permitir la aplicación de las medidas previstas en los párrafos 1 y 2.

5. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.

Título 5 – Recogida en tiempo real de datos informáticos

Artículo 20 – Recogida en tiempo real de datos informáticos

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para:

a. recoger o grabar mediante la aplicación de medios técnicos existentes en su territorio;

b. obligar a un prestador de servicios, en el ámbito de sus capacidades técnicas existentes, a

i. recoger o grabar mediante la aplicación de medios técnicos existentes en su territorio, o

ii. prestar a las autoridades competentes su colaboración y su asistencia para recopilar o grabar, en tiempo real, los datos de tráfico asociados a comunicaciones específicas transmitidas en su territorio a través de un sistema informático.

2. Cuando un Estado, en razón de los principios establecidos en su ordenamiento jurídico interno, no pueda adoptar las medidas enunciadas en el párrafo 1 (a), podrá, en su lugar, adoptar otras medidas legislativas o de otro tipo que estime necesarias para asegurar la recogida o la grabación en tiempo real de los datos de tráfico asociados a comunicaciones específicas transmitidas en su territorio mediante la aplicación de medios técnicos existentes en ese territorio.

3. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para obligar a un prestador de servicios a mantener en secreto la adopción de las medidas previstas en el presente artículo, así como cualquier información al respecto.

4. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.

Artículo 21 – Interceptación de datos relativos al contenido

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades

competentes respecto a infracciones consideradas graves conforme a su derecho interno para:

a. recoger o grabar mediante la aplicación de medios técnicos existentes en su territorio; y

b. obligar a un prestador de servicios, en el ámbito de sus capacidades técnicas existentes, a

i. recoger o grabar mediante la aplicación de medios técnicos existentes en su territorio, o

ii. prestar a las autoridades competentes su colaboración y su asistencia para recopilar o grabar, en tiempo real, los datos relativos al contenido de concretas comunicaciones en su territorio, transmitidas a través de un sistema informático.

2. Cuando un Estado, en razón de los principios establecidos en su ordenamiento jurídico interno, no pueda adoptar las medidas enunciadas en el párrafo 1 (a), podrá, en su lugar, adoptar otras medidas legislativas o de otro tipo que estime necesarias para asegurar la recogida o la grabación en tiempo real de los datos relativos al contenido de concretas comunicaciones transmitidas en su territorio mediante la aplicación de medios técnicos existentes en ese territorio.

3. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para obligar a un prestador de servicios a mantener en secreto la adopción de las medidas previstas en el presente artículo, así como cualquier información al respecto.

4. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.

Sección 3 – Competencia

Artículo 22 – Competencia

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para atribuirse la competencia respecto a cualquier infracción penal establecida en los artículos 2 a 11 del presente Convenio, cuando la infracción se haya cometido:

a. en su territorio;

b. a bordo de una nave que ondee pabellón de ese Estado;

c. a bordo de una aeronave inmatriculada en ese Estado;

d. por uno de sus súbditos, si la infracción es punible penalmente en el lugar donde se ha cometido o si la infracción no pertenece a la competencia territorial de ningún Estado.

2. Las Partes podrán reservarse el derecho de no aplicar, o de aplicar sólo en ciertos casos o condiciones específicas, las reglas de competencia definidas en los párrafos 1b a 1d del presente artículo o en cualquiera de las partes de esos párrafos.

3. Las Partes adoptarán las medidas que se estimen necesarias para atribuirse la competencia respecto de cualquier infracción mencionada en el artículo 24, párrafo 1 del presente Convenio, cuando el presunto autor de la misma se halle en su territorio y no pueda ser extraditado a otro Estado por razón de la nacionalidad, después de una demanda de extradición.

4. El presente Convenio no excluye ninguna competencia penal ejercida por un Estado conforme a su derecho interno.

5. Cuando varios Estados reivindiquen una competencia respecto a una infracción descrita en el presente Convenio, los Estados implicados se reunirán, cuando ello sea oportuno, a fin de decidir cuál de ellos está en mejores condiciones para ejercer la persecución.

Capítulo III – Cooperación internacional

Sección 1 – Principios generales

Título 1 – Principios generales relativos a la cooperación internacional

Artículo 23 – Principios generales relativos a la cooperación internacional

Las Partes cooperarán con arreglo a lo dispuesto en el presente capítulo, aplicando para ello los instrumentos internacionales relativos a la cooperación internacional en materia penal, acuerdos basados en la legislación uniforme o recíproca y en su propio derecho nacional, de la forma más amplia posible, con la finalidad de investigar los procedimientos concernientes a infracciones penales vinculadas a sistemas y datos informáticos o para recoger pruebas electrónicas de una infracción penal.

Título 2 – Principios relativos a la extradición

Artículo 24 – Extradición

1.a. El presente artículo se aplicará a la extradición por alguna de las infracciones definidas en los artículos 2 a 11 del presente Convenio, siempre que éstas resulten punibles por la legislación de los dos Estados implicados y tengan prevista una pena privativa de libertad de una duración mínima de un año.

. b. Aquellos Estados que tengan prevista una pena mínima distinta, derivada de un tratado de extradición aplicable a dos o más Estados, comprendido en la Convención Europea de Extradición (STE nº 24), o de un acuerdo basado en la legislación uniforme o recíproca, aplicarán la pena mínima prevista en esos tratados o acuerdos

2. Las infracciones penales previstas en el apartado 1 del presente artículo podrán dar lugar a extradición si entre los dos Estados existe un tratado de extradición. Las Partes se comprometerán a incluirlas como tales infracciones susceptibles de dar lugar a extradición en todos los tratados de extradición que puedan suscribir.

3. Si un Estado condiciona la extradición a la existencia de un tratado y recibe una demanda de extradición de otro Estado con el que no ha suscrito tratado alguno de extradición, podrá considerar el presente Convenio fundamento jurídico suficiente para conceder la extradición por alguna de las infracciones penales previstas en el párrafo 1 del presente artículo.

4. Las Partes que no condicionen la extradición a la existencia de un tratado podrán llevar a cabo la extradición siempre que prevean como infracciones las previstas en el párrafo 1 del presente artículo.

5. La extradición quedará sometida a las condiciones establecidas en el derecho interno del Estado requerido o en los tratados de extradición vigentes, quedando asimismo sometidos a estos instrumentos jurídicos los motivos por los que el país requerido puede denegar la extradición.

6. Si es denegada la extradición por una infracción comprendida en el párrafo 1 del presente artículo, alegando la nacionalidad de la persona reclamada o la competencia para juzgar la infracción del Estado requerido, éste deberá someter el asunto –la demanda del Estado requirente —a sus autoridades competentes a fin de que éstas establezcan la competencia para perseguir el hecho e informen de la conclusión alcanzada al Estado requirente. Las autoridades en cuestión deberán adoptar la decisión y sustanciar el procedimiento del mismo modo que para el resto de infracciones de naturaleza semejante previstas en la legislación de ese Estado.

7.a. Las Partes deberán comunicar al Secretario General del Consejo de Europa, en el momento de la firma o del depósito del instrumento de ratificación, aceptación, aprobación o adhesión, el nombre y la dirección de las autoridades responsables del envío y de la recepción de una demanda de extradición o de arresto provisional, en caso de ausencia de tratado.

b. El Secretario General del Consejo de Europa creará y actualizará un registro de autoridades designadas por las Partes. Las Partes deberán garantizar la exactitud de los datos obrantes en el registro

Título 3 – Principios generales relativos a la colaboración [8]

Artículo 25 – Principios generales relativos a la colaboración

1. Las Partes acordarán llevar a cabo una colaboración mutua lo más amplia posible al objeto de investigar los procedimientos concernientes a infracciones penales vinculadas a sistemas y datos informáticos o al de recoger pruebas electrónicas de una infracción penal.

2. Las Partes adoptarán las medidas legislativas o de otro tipo que estimen necesarias para dar cumplimiento a las obligaciones establecidas en los artículos 27 a 35.

3. Las Partes podrán, en caso de emergencia, formular una demanda de colaboración, a través de un medio de comunicación rápido, como el fax o el correo electrónico, procurando que esos medios ofrezcan las condiciones suficientes de seguridad y de autenticidad (encriptándose si fuera necesario) y con confirmación posterior de la misma si el Estado requerido lo exigiera. Si el Estado requerido lo acepta podrá responder por cualquiera de los medios rápidos de comunicación indicados.

4. Salvo disposición en contrario expresamente prevista en el presente capítulo, la colaboración estará sometida a las condiciones fijadas en el derecho interno del Estado requerido o en los tratados de colaboración aplicables y comprenderá los motivos por los que el Estado requerido puede negarse a colaborar. El Estado requerido no podrá ejercer su derecho a rehusar la colaboración en relación a las infracciones previstas en los artículos 2 a 11, alegando que la demanda se solicita respecto a una infracción que, según su criterio, tiene la consideración de fiscal.

5. Conforme a lo dispuesto en el presente capítulo, el Estado requerido estará autorizado a supeditar la colaboración a la exigencia de doble incriminación. Esa condición se entenderá cumplida si el comportamiento constitutivo de la infracción - en relación a la que se solicita la colaboración — se encuentra previsto en su derecho interno como infracción penal, resultando indiferente que éste no la encuadre en la misma categoría o que no la designe con la misma terminología.

Artículo 26 – Información espontánea

1. Las Partes podrán, dentro de los límites de su derecho interno y en ausencia de demanda previa, comunicar a otro Estado las informaciones obtenidas en el marco de investigaciones que puedan ayudar a la Parte destinataria a iniciar o a concluir satisfactoriamente las investigaciones o procedimientos relativos a las infracciones dispuestas en el presente Convenio, o a que dicha parte presente una demanda de las previstas en el presente capítulo.

2. Antes de comunicar dicha información, ese Estado podrá solicitar que la información sea tratada de forma confidencial o que sea utilizada sólo en ciertas circunstancias. Si el Estado destinatario no pudiera acatar las condiciones impuestas, deberá informar al otro Estado, quien habrá de decidir si proporciona o no la información. Una vez aceptadas estas condiciones por el Estado destinatario, éste quedará obligado a su cumplimiento.

Título 4 – Procedimientos relativos a las demandas de asistencia en ausencia de acuerdo internacional aplicable

Artículo 27 – Procedimiento relativo a las demandas de colaboración en ausencia de acuerdo internacional aplicable

1. En ausencia de tratado o acuerdo en vigor de asistencia basado en la legislación uniforme o recíproca, serán aplicables los apartados 2 al 9 del presente artículo. Éstos no se aplicarán cuando exista un tratado, acuerdo o legislación sobre el particular, sin perjuicio de que las partes implicadas puedan decidir someterse, en todo o parte, a lo dispuesto en este artículo.

2.a. Las Partes designarán una o varias autoridades centrales encargadas de tramitar las demandas de colaboración, de ejecutarlas o de transferirlas a las autoridades competentes para que éstas las ejecuten.

b. Las autoridades centrales se comunicarán directamente las unas con las otras.

c. Las Partes, en el momento de la firma o del depósito de sus instrumentos de ratificación, aceptación, de aprobación o de adhesión, comunicarán al Secretario General del Consejo de Europa los nombres y direcciones de las autoridades designadas en aplicación del presente párrafo.

d. El Secretario General del Consejo de Europa creará y actualizará un registro de autoridades designadas por las partes. Las Partes deberán garantizar la exactitud de los datos obrantes en el registro.

3. Las demandas de asistencia basadas en el presente artículo serán ejecutadas conforme al procedimiento especificado por el Estado requirente, siempre que resulte compatible con la legislación del Estado requerido.

4. Al margen de los motivos previstos en el artículo 15 párrafo 4 para denegar la asistencia, ésta podrá ser rechazada por el Estado requerido:

a. si la demanda se refiere a una infracción que el Estado requerido considera de naturaleza política o vinculada a una información de naturaleza política o;

b. si el Estado requerido estima que, de acceder a la colaboración, se pondría en peligro su soberanía, seguridad, orden público u otro interés esencial.

5. El Estado requerido podrá aplazar la ejecución de la demanda cuando ésta pueda perjudicar investigaciones o procedimientos en curso llevados a cabo por las autoridades nacionales.

6. Antes de denegar o retrasar la asistencia, el Estado requerido deberá examinar, tras consultar al Estado requirente, si es posible hacer frente a la demanda de forma parcial o si es posible establecer las reservas que estime necesarias.

7. El Estado requerido informará inmediatamente al Estado requirente del curso que pretende dar a la demanda de asistencia. De denegar o retrasar la tramitación de la demanda, el Estado requerido hará constar los motivos. Asimismo, dicho Estado deberá informar al Estado requirente sobre los motivos que hacen imposible, de ser así, la ejecución de la demanda o que retrasan sustancialmente su ejecución.

8. El Estado requirente podrá solicitar que el Estado requerido mantenga en secreto la propia existencia y objeto de la demanda interpuesta al amparo de este capítulo, salvo en aquellos aspectos necesarios para la ejecución de la misma. Si el Estado requirente no pudiera hacer frente a la petición de confidencialidad, éste deberá informar inmediatamente al otro Estado, quien decidirá si la demanda, pese a ello, debe ser ejecutada.

9.a. En caso de urgencia, las autoridades judiciales del Estado requirente podrán dirigir directamente a las autoridades homólogas del Estado requerido las demandas de asistencia y las comunicaciones. En tales casos, se remitirá simultáneamente una copia a las autoridades del Estado requerido con el visado de la autoridad central del Estado requirente.

b. Todas las demandas o comunicaciones formuladas al amparo del presente parágrafo podrán ser tramitadas a través de la Organización Internacional de la Policía Criminal (INTERPOL).

c. Cuando una demanda haya sido formulada al amparo de la letra (a) del presente artículo, y la autoridad que le dio curso no sea la competente para ello, deberá transferir la demanda a la autoridad nacional competente y ésta informará directamente al Estado requerido.

d. Las demandas o comunicaciones realizadas al amparo del presente párrafo que no supongan la adopción de medidas coercitivas podrán ser tramitadas directamente por las autoridades del Estado requirente y las del Estado requerido.

e. Las Partes podrán informar al Secretario General del Consejo de Europa, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, que, por motivos de eficacia, las demandas formuladas al amparo del presente párrafo deberán dirigirse directamente a su autoridad central.

Artículo 28 – Confidencialidad y restricciones de uso

1. En ausencia de tratado o acuerdo en vigor de asistencia basados en la legislación uniforme o recíproca, será aplicable lo dispuesto en el presente artículo. Éste no se aplicará cuando exista un tratado, acuerdo o legislación sobre el particular, sin perjuicio de que las partes implicadas puedan decidir someterse, en todo o parte, a lo dispuesto en este artículo.

2. El Estado requerido podrá supeditar la comunicación de la información o del material requerido en la demanda al cumplimiento de las siguientes condiciones:

a. que se mantenga la confidencialidad sobre las mismas, siempre que la demanda corra el riesgo fracasar en ausencia de dicha condición; o

b. que éstas no sean utilizadas en investigaciones o procedimientos diversos a los establecidos en la demanda.

3. Si el Estado requirente no pudiera satisfacer alguna de las condiciones establecidas en el apartado 2 del presente artículo, la otra parte informará al Estado requerido, el cual decidirá si la información debe ser proporcionada. Si el Estado requirente acepta esta condición, dicho Estado estará obligado por la misma.

4. Todo Estado parte que aporte información o material supeditado a alguna de las condiciones previstas en el apartado 2, podrá exigir de la otra parte la concreción de las condiciones de uso de la información o del material.

Sección 2 – Disposiciones específicas

Título 1 – Cooperación en materia de medidas cautelares

Artículo 29 – Conservación inmediata datos informáticos almacenados

1. Las Partes podrán ordenar o imponer de otro modo la conservación inmediata de datos almacenados en sistemas informáticos que se encuentren en su territorio, en relación a los cuales el Estado requirente tiene intención de presentar una demanda de asistencia para registrar o acceder de otro modo, decomisar u obtener por otro medio, o lograr la comunicación de dichos datos.

2. Una demanda de conservación formulada en aplicación del párrafo 1 deberá contener:

a. la identificación de la autoridad que solicita la conservación;

b. la infracción objeto de investigación con una breve exposición de los hechos vinculados a la misma;

c. los datos informáticos almacenados que deben conservarse y su vinculación con la infracción;

d. todas aquellas informaciones disponibles que permitan identificar al responsable de los datos informáticos almacenados o el emplazamiento de los sistemas informáticos;

e. justificación de la necesidad de conservación; y

f. la acreditación de que el Estado requirente está dispuesto a formular una demanda de asistencia para registrar o acceder de otro modo, decomisar u obtener por otro medio, o lograr la comunicación de dichos datos.

3. Después de recibir la demanda, el Estado requerido deberá adoptar las medidas necesarias para proceder sin dilaciones a la conservación de los datos solicitados, conforme a su derecho interno. Para hacer efectiva la demanda de conservación no resultará condición indispensable la doble incriminación.

4. Si un Estado exige la doble incriminación como condición para atender a una demanda de asistencia para registrar o acceder de otro modo, decomisar u obtener por otro medio, o lograr la comunicación de dichos datos, por infracciones diversas a las establecidas en los artículos 2 a 11 del presente Convenio, podrá negarse a la demanda de conservación, al amparo del presente artículo, si tiene fundadas sospechas de que, en el momento de la comunicación de los datos, el otro Estado no cumplirá la exigencia de la doble incriminación.

5. Al margen de lo anterior, una demanda de conservación únicamente podrá ser denegada:

a. si la demanda se refiere a una infracción que el Estado requerido considera de naturaleza política o vinculada a una información de naturaleza política o;

b. si el Estado requerido estima que de acceder a la demanda se pondría en peligro su soberanía, su seguridad, orden público u otro interés esencial.

6. Cuando el Estado requerido considere que la simple conservación no será suficiente para garantizar la disponibilidad futura de los datos informáticos o que ésta podría comprometer la confidencialidad de la investigación o podría hacerla fracasar de otro modo, deberá informar inmediatamente al Estado requirente, quien decidirá la conveniencia de dar curso a la demanda.

7. Todas las conservaciones realizadas al amparo de una demanda de las previstas en el párrafo 1 serán válidas por un periodo máximo de 60 días, para permitir, en ese plazo de tiempo, al Estado requirente formular una demanda de asistencia para registrar o acceder de otro modo, decomisar u obtener por otro medio, o lograr la comunicación de dichos datos. Después de la recepción de la demanda, los datos informáticos deberán mantenerse hasta que ésta se resuelva.

Artículo 30 – Comunicación inmediata de los datos informáticos conservados

1. Si, en ejecución de una demanda de conservación de datos de tráfico relativos a una concreta comunicación al amparo del artículo 29, el Estado requerido descubriera que un prestador de servicios de otro Estado ha participado en la transmisión de la comunicación, comunicará inmediatamente al Estado requirente los datos informáticos de tráfico, con el fin de que éste identifique al prestador de servicios y la vía por la que la comunicación ha sido realizada.

2. La comunicación de datos informáticos de tráfico prevista en el párrafo 1 únicamente podrá ser denegada:

a. si la demanda se refiere a una infracción que el Estado requerido considera de naturaleza política o vinculada a una información de naturaleza política o;

b. si el Estado requerido estima que de acceder a la demanda se pondría en peligro su soberanía, su seguridad, orden público o otro interés esencial.

Título 2 – Asistencia en relación a los poderes de investigación

Artículo 31 – Asistencia concerniente al acceso a datos informáticos almacenados

1. Cualquier Estado podrá solicitar a otro el registro o acceso de otro modo, el decomiso u obtención por otro medio, o la comunicación de datos almacenados en un sistema informático que se encuentre en su territorio, incluidos los datos conservados conforme a lo dispuesto en el artículo 29.

2. El Estado requerido dará satisfacción a la demanda aplicando los instrumentos internacionales, convenios y la legislación mencionada en el artículo 23 siempre que no entre en contradicción con lo dispuesto en el presente capítulo.

3. La demanda deberá ser satisfecha lo más rápidamente posible en los siguientes casos:

a. cuando existan motivos para sospechar que los datos solicitados son particularmente vulnerables por existir riesgo de pérdida o modificación; o

b. cuando los instrumentos, convenios o legislación referida en el párrafo 2 prevean una cooperación rápida.

Artículo 32 – Acceso transfronterizo a los datos informáticos almacenados, con consentimiento o de libre acceso

Cualquier Estado podrá sin autorización de otro:

a. acceder a los datos informáticos almacenados de libre acceso al público (fuentes abiertas), independientemente de la localización geográfica de esos datos; o

b. acceder a, o recibir a través de un sistema informático situado en su territorio, los datos informáticos almacenados situados en otro Estado, si se obtiene el consentimiento legal y voluntario de la persona autorizada para divulgarlos a través de ese sistema informático.

Artículo 33 – Asistencia para la recogida en tiempo real de datos de tráfico

1. Las Partes podrán acordar colaborar en la recogida, en tiempo real, de datos de tráfico, asociados a concretas comunicaciones llevadas a cabo en sus territorios, a través un sistema informático. Dicha colaboración se someterá a las condiciones y procedimientos previstos en el derecho interno, salvo que alguna de las partes se acoja a la reserva prevista en el párrafo 2.

2. Las Partes deberán acordar colaborar respecto a aquellas infracciones penales para las cuales la recogida en tiempo real de datos de tráfico se encuentra prevista en su derecho interno en situaciones análogas.

Artículo 34 – Asistencia en materia de interceptación de datos relativos al contenido

Las Partes podrán acordar colaborar, en la medida en que se encuentre previsto por tratados o leyes internas, en la recogida y registro, en tiempo real, de datos relativos al contenido de concretas comunicaciones realizadas a través de sistemas informáticos.

Título 3 – Red 24/7

Artículo 35 – Red 24/7

1. Las Partes designarán un punto de contacto localizable las 24 horas del día, y los siete días de la semana, con el fin de asegurar la asistencia inmediata en la investigación de infracciones penales llevadas a cabo a través de sistemas y datos informáticos o en la recogida de pruebas electrónicas de una infracción penal. Esta asistencia comprenderá, si lo permite el derecho y la práctica interna, facilitar la aplicación directa de las siguientes medidas:

a. aportación de consejos técnicos;

b. conservación de datos según lo dispuesto en los artículos 29 y 30; y

c. recogida de pruebas, aportación de información de carácter jurídico y localización de sospechosos.

2.a. Un mismo punto de contacto podrá ser coincidente para dos Estados, siguiendo para ello un procedimiento acelerado.

b. Si el punto de contacto designado por un Estado no depende de su autoridad o autoridades responsables de la colaboración internacional o de la extradición, deberá velarse para que ambas autoridades actúen coordinadamente mediante la adopción de un procedimiento acelerado.

3. Las Partes dispondrán de personal formado y dotado a fin de facilitar el funcionamiento de la red.

Consideramos que la Convención de Budapest en temas de Cibercrimen, es una herramienta la cual el Perú debería adoptar, pero claro, esto atendiendo a el más sincero proceso de adaptación a nuestra realidad, y siempre buscando la innovación en la materia, como es el caso de Guatemala, que ha

regulado el tema informático, así como cibernético, con lo cual se podría dar la posibilidad de que con la sola intención de Ciberdelincuente, se esté generando la comisión de un ilícito penal.

"Programas Destructivos

Artículo 36: 1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar la posibilidad de detectar la comercialización o aplicación dentro de algún sistema informático o cibernético con programas destructivos que puedan causar perjuicio a los registros, programas o equipos de computación dentro del ciberespacio o en el territorio nacional.

ANALISIS DE IMPACTO REGULATORIO EX–ANTE O EX–POST:

Elección de una herramienta regulatoria a partir del Análisis de Impacto Regulatorio del Proyecto de Ley de Ciberdelitos, basado en el Convenio de Budapest sobre Cibercriminalidad

Rafael Parra Perea

1. INTRODUCCIÓN

A partir del siglo XX, una revolución tecnológica empezó a desarrollarse de manera desmesurada, colocando nuevos espacio de comunicación e intercambio de información al alcance de todo el que podía tener acceso a ella. Con esta revolución de las Tecnologías de la Información y las Comunicaciones – TICs, nuevas formas de desarrollar diversos ámbitos de la vida cotidiana del ser humano se ven relación íntegramente con el Ciber espacio, lo cual ha generado que los las personas puedan realizar diversas actividades con solo presionar un botón.

El constante desarrollo de las TICs es un punto que como comunidad nos ha beneficiado pero el crecimiento ha sido tan exponencial que cuando empezamos a recapacitar en la seguridad ya nos habíamos hecho dependientes de esta nueva forma de intercambiar información, con lo cual nos queda aprender y seguir mejorando nuestros sistemas de seguridad tanto en materia Informática como en materia Cibernética.

En definitiva, no es difícil imaginar que la experiencia Peruana en materia de ciber incidentes es mínima si nos comparamos con la gran cantidad de ataques que han sufrido otro países de la comunidad internacional, esto no quiere decir que el Perú, se encuentre en una situación en cual no pueda resultar ser víctima de un ataque cibernético o informático, es por ellos que la situación nos hace tener que tomar una decisión sobre la marcha y comenzar a implementar herramientas, pero no solo es necesario implementar herramientas, sino analizar el tipo de herramientas que se deberían implementar y que tipo de control deben de aplicar, si bien debe ser un control tipo ex – ante, a toda actividad existente en el mercado - de alcance limitado hasta hoy al sector informático-, y como mecanismo complementario al ya vigente control de conductas o control de tipo ex-post, regulado por la actual ley de protección de dato personales (*Ley 29733)* así como la ley que incorpora los delitos informáticos en el código penal (Ley 30096).

El presente documento, lejos de mostrarse a priori en favor de uno u otro, pretende mostrar los resultados alcanzados a través del uso del Análisis de Impacto Regulatorio (AIR), como una de las herramientas que, aplicadas durante más de veinte años en diversos países del mundo, goza de reconocimiento con la finalidad de cuidar la calidad de las normas legales, y

con ello, lograr los objetivos trazados, al menor costo posible y con los menores efectos negativos indeseados.

Al hacer referencia al Análisis de Impacto Regulatorio, QUINTANA señala que "(…) su finalidad destacada es dar un enfoque más racional para la elaboración de normas legales, a través de una metodología que se ha venido estandarizando y aplicando en distintas realidades y países.". A partir de lo indicado por QUINTANA, y siguiendo lo planteado por BARRANTES, el AIR se compone de tres etapas, las cuales se indican a continuación:

1. Identificación del Problema y Definición de los Objetivos, que consiste en determinar el problema que se considera necesario solucionar a través de la intervención del Estado.
2. Identificación de Opciones Regulatorias.
3. Valorización y Comparación de Opciones Regulatorias, dentro del cual se encuentra el análisis costo beneficio

Ahora bien, ya habiendo identificado el estado en el que se encuentra nuestra realidad nacional, y buscando mostrar los resultados de la aplicación de la metodología AIR al caso específico, utilizando, como ya mencionamos, la base del Convenio de Budapest sobre Ciberciminalidad del 2001.

2. PROYECTO DE LEY

El Proyecto de Ley presentado hace necesario plantear la evaluación previa de los actos de concentración empresariales y Estatales que produzcan o puedan producir efectos negativos directos o que pueden generar un situación favorable para que se produzcan dichos efectos negativos, en todo o parte del territorio nacional, aun cuando se hayan originado en el extranjero (artículo 24°), estableciendo los supuestos de colaboración entre los Estados tratantes, así como las acciones ocurridas dentro del territorio nacional del Estado Peruanos (artículo 22°), en cualquiera de los siguientes supuestos:

Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para atribuirse la competencia respecto a cualquier infracción penal establecida en los artículos 2 a 11 del presente Convenio, cuando la infracción se haya cometido:

a. en su territorio;

b. a bordo de una nave que ondee pabellón de ese Estado;

c. a bordo de una aeronave inmatriculada en ese Estado;

d. por uno de sus súbditos, si la infracción es punible penalmente en el lugar donde se ha cometido o si la infracción no pertenece a la competencia territorial de ningún Estado.

Definido lo que la "competencia territorial" en materia informática y cibernética es, entonces podemos determinar que el convenio establece un umbral de tipo cualitativo relacionado a la condición del agente accionante, dándose la posibilidad de que el agente sea Peruano o no y que éste se encuentre dentro o no del territorio nacional.

Este umbral de competencia territorial, abre la posibilidad de la cooperación internacional en materia de extradición, pero esto bajo estrictos parámetros previamente acordados entre países.

Artículo 24 – Extradición

1. a. El presente artículo se aplicará a la extradición por alguna de las infracciones definidas en los artículos 2 a 11 del presente Convenio, siempre que éstas resulten punibles por la legislación de los dos Estados implicados y tengan prevista una pena privativa de libertad de una duración mínima de un año.

2. Las infracciones penales previstas en el apartado 1 del presente artículo podrán dar lugar a extradición si entre los dos Estados existe un tratado de extradición. Las Partes se comprometerán a incluirlas como tales infracciones susceptibles de dar lugar a extradición en todos los tratados de extradición que puedan suscribir.

3. Si un Estado condiciona la extradición a la existencia de un tratado y recibe una demanda de extradición de otro Estado con el que no ha suscrito tratado alguno de extradición, podrá considerar el presente Convenio fundamento jurídico suficiente para conceder la extradición por alguna de las infracciones penales previstas en el párrafo 1 del presente artículo.

4. Las Partes que no condicionen la extradición a la existencia de un tratado podrán llevar a cabo la extradición siempre que prevean como infracciones las previstas en el párrafo 1 del presente artículo.

5. La extradición quedará sometida a las condiciones establecidas en el derecho interno del Estado requerido o en los tratados de extradición vigentes, quedando asimismo sometidos a estos instrumentos jurídicos los motivos por los que el país requerido puede denegar la extradición.

6. Si es denegada la extradición por una infracción comprendida en el párrafo 1 del presente artículo, alegando la nacionalidad de la persona reclamada o la competencia para juzgar la infracción del Estado requerido, éste deberá someter el asunto – la demanda del Estado requirente —a sus autoridades competentes a fin de que éstas establezcan la competencia para perseguir el hecho e informen de la conclusión alcanzada al Estado requirente. Las autoridades en cuestión deberán adoptar la decisión y sustanciar el procedimiento del mismo modo que para el resto de infracciones de naturaleza semejante previstas en la legislación de ese Estado.

Se hace necesario, que al momento plantear la extradición la administración pública, tenga en claro lo mencionado en el artículo 24 inciso "a", que son los artículos del 2 al 11.

Capítulo II – Medidas que deben ser adoptadas a nivel nacional

Sección 1 – Derecho penal material

Título 1 – Infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

Artículo 2 – Acceso ilícito

Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, el acceso doloso y sin autorización a todo o parte de un sistema informático. Las Partes podrán exigir que la infracción sea cometida con vulneración de medidas de seguridad, con la intención de obtener los datos informáticos o con otra intención delictiva, o también podrán requerir que la infracción se perpetre en un sistema informático conectado a otro sistema informático.

Artículo 3 – Interceptación ilícita

Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la interceptación, dolosa y sin autorización, cometida a través de medios técnicos, de datos informáticos – en transmisiones no públicas– en el destino, origen o en el interior de un sistema informático, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporta tales datos informáticos. Las Partes podrán exigir que la infracción sea cometida con alguna intención delictiva o también podrán requerir que la infracción se perpetre en un sistema informático conectado a otro sistema informático.

Artículo 4 – Atentados contra la integridad de los datos

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la conducta de dañar, borrar, deteriorar, alterar o suprimir dolosamente y sin autorización los datos informáticos.

2. Las Partes podrán reservarse el derecho a exigir que el comportamiento descrito en el párrafo primero ocasione daños que puedan calificarse de graves.

Artículo 5 – Atentados contra la integridad del sistema

Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la obstaculización grave, cometida de forma dolosa y sin autorización, del funcionamiento de un sistema informático, mediante la introducción,

transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.

Artículo 6 – Abuso de equipos e instrumentos técnicos

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, las siguientes conductas cuando éstas sean cometidas dolosamente y sin autorización:

a. la producción, venta, obtención para su utilización, importación, difusión u otras formas de puesta a disposición:

i. de un dispositivo, incluido un programa informático, principalmente concebido o adaptado para permitir la comisión de una de las infracciones establecidas en los artículos 2 a 5 arriba citados;

ii. de una palabra de paso (contraseña), de un código de acceso o de datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con la intención de utilizarlos como medio para cometer alguna de las infracciones previstas en los artículos 2 a 5; y

b. la posesión de alguno de los elementos descritos en los parágrafos (a) (1) o (2) con la intención de utilizarlos como medio para cometer alguna de las infracciones previstas en los artículos 2-5. Los Estados podrán exigir en su derecho interno que concurra un determinado número de elementos para que nazca responsabilidad penal.

2. Lo dispuesto en el presente artículo no generará responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, difusión u otras formas de puesta a disposición mencionadas en el párrafo 1 no persigan la comisión de una infracción prevista en los artículos 2 a 5 del presente Convenio, como en el caso de ensayos autorizados o de la protección de un sistema informático.

3. Las Partes podrán reservarse el derecho de no aplicar el párrafo 1, a condición de que dicha reserva no recaiga sobre la venta, distribución o cualesquiera otras formas de puesta a disposición de los elementos mencionados en el parágrafo 1 (a) (2).

Título 2 – Infracciones informáticas

Artículo 7 – Falsedad informática

Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal,

conforme a su derecho interno, la introducción, alteración, borrado o supresión dolosa y sin autorización de datos informáticos, generando datos no auténticos, con la intención de que sean percibidos o utilizados a efectos legales como auténticos, con independencia de que sean directamente legibles e inteligibles. Las Partes podrán reservarse el derecho a exigir la concurrencia de un ánimo fraudulento o de cualquier otro ánimo similar para que nazca responsabilidad penal.

Artículo 8 – Estafa informática

Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la producción de un perjuicio patrimonial a otro, de forma dolosa y sin autorización, a través de:

a. la introducción, alteración, borrado o supresión de datos informáticos,

b. cualquier forma de atentado al funcionamiento de un sistema informático, con la intención, fraudulenta o delictiva, de obtener sin autorización un beneficio económico para sí mismo o para tercero.

Título 3 – Infracciones relativas al contenido

Artículo 9 – Infracciones relativas a la pornografía infantil

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, las siguientes conductas cuando éstas sean cometidas dolosamente y sin autorización:

a. la producción de pornografía infantil con la intención de difundirla a través de un sistema informático;

b. el ofrecimiento o la puesta a disposición de pornografía infantil a través de un sistema informático;

c. la difusión o la transmisión de pornografía infantil a través de un sistema informático;

d. el hecho de procurarse o de procurar a otro pornografía infantil a través de un sistema informático;

e. la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos.

2. A los efectos del párrafo 1 arriba descrito, la «pornografía infantil» comprende cualquier material pornográfico que represente de manera visual:

a. un menor adoptando un comportamiento sexualmente explícito;

b. una persona que aparece como un menor adoptando un comportamiento sexualmente explícito;

c. unas imágenes realistas que representen un menor adoptando un comportamiento sexualmente explícito.

3. A los efectos del párrafo 2 arriba descrito, el término «menor» designa cualquier persona menor de 18 años. Las Partes podrán exigir un límite de edad inferior, que debe ser como mínimo de 16 años.

4. Los Estados podrán reservarse el derecho de no aplicar, en todo o en parte, los párrafos 1 (d) y 1 (e) y 2 (b) y 2 (c).

Título 4 – Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines

Artículo 10 – Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, los atentados a la propiedad intelectual definida por la legislación de cada Estado, conforme a las obligaciones que haya asumido por aplicación de la Convención Universal sobre los Derechos de Autor, revisada en París el 24 de julio de 1971, del Convenio de Berna para la protección de obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Derecho de Autor, a excepción de cualquier derecho moral conferido por dichas Convenciones, cuando tales actos sean cometidos deliberadamente, a escala comercial y a través de un sistema informático.

2. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, los atentados a los derechos afines definidos por la legislación de cada Estado, conforme a las obligaciones que haya asumido por aplicación de la Convención Internacional sobre la Protección de los Artistas Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión, hecha en Roma (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre interpretación o ejecución y fonogramas, a excepción de cualquier derecho moral conferido por dichas Convenciones, cuando tales actos sean cometidos deliberadamente, a escala comercial y a través de un sistema informático.

3. Las Partes podrán, de concurrir determinadas circunstancias, reservarse el derecho de no imponer responsabilidad penal en aplicación de los párrafos 1 y 2 del presente artículo, siempre que se disponga de otros recursos eficaces para su represión y que dicha reserva no comporte infracción de las obligaciones internacionales que incumban al Estado por aplicación de los instrumentos internacionales mencionados en los párrafos 1 y 2 del presente artículo.

Título 5 – Otras formas de responsabilidad y sanción

Artículo 11 – Tentativa y complicidad

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, cualquier acto de complicidad que sea cometido dolosamente y con la intención de favorecer la perpetración de alguna de las infracciones establecidas en los artículos 2 a 10 del presente Convenio.

2. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la tentativa dolosa de cometer una de las infracciones establecidas en los artículos 3 a 5, 7, 8, 9 (1) a y 9 (1) c del presente Convenio.

3. Las Partes podrán reservarse el derecho de no aplicar, en todo o en parte, el párrafo 2 del presente artículo.

Lo mostrado por el Convenio de Budapest son los tipos penales especifico por los cuales la Administración Publica podría solicitar la extradición de algún agente que se encuentre fue del territorio nacional, el cual es requerido por las autoridades nacionales por la comisión de alguno de estos tipos penales.

El Convenio de Budapest hace extensiva la participación en la comisión de delitos informáticos y cibernéticos a la personas jurídicas, si bien con las hace susceptibles de ser extraditadas, nos abre la posibilidad de que la persona jurídica sea tenida como responsable.

Artículo 12 – Responsabilidad de las personas jurídicas

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para permitir que las personas jurídicas puedan ser tenidas por responsables de las infracciones establecidas en el presente Convenio, cuando éstas sean cometidas por una persona física, actuando ya sea a título individual, ya sea como miembro de un órgano de la persona jurídica, que ejerce un poder de dirección en su seno, cuyo origen se encuentre en:

a. un poder de representación de la persona jurídica;

b. una autorización para tomar decisiones en nombre de la persona jurídica;

c. una autorización para ejercer control en el seno de la persona jurídica.

2. Fuera de los casos previstos en el párrafo 1, las Partes adoptarán las medidas necesarias para asegurar que una persona jurídica puede ser tenida por responsable cuando la ausencia de vigilancia o de control por parte de cualquier persona física mencionada en el párrafo 1 haya permitido la comisión de las infracciones descritas en el párrafo 1 a través de una persona física que actúa bajo autorización de la persona jurídica.

3. La responsabilidad de la persona jurídica podrá resolverse en sede penal, civil o administrativa, dependiendo de los principios jurídicos propios del Estado.

4. Esta responsabilidad se establecerá sin perjuicio de la responsabilidad penal de las personas físicas que hayan cometido la infracción.

3. EL CONTROL DE TIPO EX-ANTE Y EL CONTROL DE TIPO EX-POST

Teniendo en cuenta lo mostrado por el Convenio, y analizando lo que implica las TICs y todo el desarrollo de las infraestructuras críticas que el Estado Peruano posee y las que están por determinarse, no se hace necesario debatir entre cuál de las dos opciones, ex – ante o ex – post, se la mejor opción, consideramos que para el presente tema se hace necesario que se ajusten las medidas necesarias tanto ex – ante como ex – post.

	Horizontal	Vertical	Conglomerado
Efectos positivos	• Se obtendrá tener un control mayor sobre las actividades ilícitas dentro del territorio nacional. • Se aplicaran los estándares internacionales a la realidad Peruana. • Se utilizara el apoyo internacional en materia de investigaciones.	• Mayor calidad en materia de seguridad cibernética e informática. • Reforzamiento de a confianza en los sistemas informáticos y cibernéticos.	•
Efectos Negativos	• -	-	-

3.1 Ex – Ante

La característica principal del control ex – ante, es el poder prevenir o generar condiciones negativas para la comisión de los tipos ilícitos, con lo cual consideramos que el Convenio de Budapest no establece los mecanismos necesario ex – antes, salvo con lo relacionado a la tentativa, para ello consideramos que una de las propuestas mejor planteadas para la realidad Peruana en materia de control ex – ante, sería la posibilidad de crear en materia seguridad "equipos rojos" que sean capaces de reaccionar de forma previa realizando el hacking ético en las redes internas de las infraestructuras cibernéticas a nivel nacional, y por otro lado a manera de control ex – ante en materia de defensa, crear un ente especializado en ciber incidentes a gran escala, que afecten la soberanía nacional, sean estos perpetrados dentro o fuera del territorio nacional.

Consideramos que como mecanismo de control ex – ante no pueden estar como entes aislados, para ambos, la comunicación e intercambio de información tiene que ser de manera fluida, los cuales puedan intercambiar la información en tiempo real para así poder aumentar la capacidad de reacción en un incidente real.

Se hace necesario establecer que a través del hacking ético a la red de las infraestructuras críticas a nivel nacional no solo se fortalece la infraestructura, sino la red completa de usuarios y proveedores de servicios.

3.2 Ex – Post

Con respecto a este tipo de control, no es necesario generar un debate, el Perú cuenta con controles de tipo Ex – Post, y el Convenio de Budapest sobre Cibercriminalidad también lo es.

La implementación de controles Ex – Post colaboraran a la represión de las conductas que sean consideradas lesivas para el ordenamiento nacional en materia cibernética e informática, por esta razón es que se hace necesario aplicar sanciones no solo de forma previa sino es necesario que una vez cometido el tipo se desarrolle la investigación pertinente tendente a determinar todas las aristas que podrían llegar a verse implicadas dentro de un ciberincidente, como por ejemplo el hecho de haber actuado de forma colectiva o individual, si forma parte de un plan en desarrollo, o si más de un sistema pudo ser afectado a causa del incidente.

Cabe resaltar que a diferencia del control de tipo Ex - Ante, que son mecanismos que en todo momento debe de encontrarse activos operando sobre las redes a cargo de la Administración Pública. Es por ello que, en caso de no contar la autoridad estatal lo suficientemente implementada con sistemas adecuados y con el personal capacitado, existe la posibilidad de que el grado de detección de conductas sea menor que en el caso de un control de tipo ex-post, en el que se debe analizar en base a un hecho en concreto realizado, principio.

3.3 Consideraciones finales

Lo planteado líneas arriba lleva a que, con independencia del ejercicio de la metodología de Análisis de Impacto Regulatorio, que representa una evaluación para un caso específico, las opciones regulatorias anteriormente analizadas, como el control de tipo ex - ante y el control de tipo ex - post, poseen beneficios y al mismo tiempo limitaciones, lo que permite pensar en una complementariedad de los instrumentos.

Como señalan TÁVARA y DIEZ CANSECO con relación a los mecanismos de control de tipo ex-ante y ex-post "(…) la evidencia disponible revela que estos dos tipos de controles son en realidad complementarios y no deben entenderse como sustitutos. El análisis de la legislación comparada muestra claramente que casi todos los países los utilizan de manera simultánea y complementaria, y que el control de conductas no sustituye al control de estructuras (…)".

No consideramos que la materia analizada permita que de acuerdo a un caso específico se determine si uno u otro es el más adecuado, esto debido a que el caso específico analizado es la realidad Peruana en materia del ciberespacio, y su correcta implementación de mecanismos jurídicos, es por ellos que la complementariedad es más que necesaria, es obligatoria.

La metodología AIR que hemos pretendido realizar lleva consigo la posibilidad de establecer si es que a través de la regulación de los ciberincidentes como afectación a la soberanía del Estado constituyen una Barrera Legal o una Barrera Burocrática.

Desde ese punto de vista la presente metodología después de analizar si la intención del Estado debería ser un control de tipo ex – ante o de tipo ex – post, es necesaria debido a la repercusión que tendría en el mercado Peruano la implementación de este tipo de controles.

Consideramos que el Estado Peruano después de todo lo analizado en la investigación debe de implementar ambos tipos de control, esto debido a las repercusiones Soberanas que implica la falta de regulación y la afectación a los intereses de los usuarios de la red dentro del Perú, que al final es traducido como las personas, grupos económicos, o desde otro punto de vista la sociedad en su totalidad.

La regulación de los ciberincidentes dentro del marco jurídico Peruano constituye una Barrera Legal favorable para el Estado, esto debido a que una vez implementada se fortalecerá no solo la defensa de los intereses soberanos del Estado, sino que se generara la conciencia positiva de los sistema informáticos y cibernéticos, y el resultado de ello, a su vez se verá reflejado en un mercado con índices de seguridad mayores los cuales favorecerán no solo al interés de defender la soberanía sino que se tendrá un mercado con mayores y mejores estándares de seguridad.

Por ende, concluimos que el AIR es favorable, y es recomendable que el Estado adopte las medidas que hemos propuesto.

3. Resultado obtenido del uso de la metodología AIR al Convenio de Budapest.

El resultado de la aplicación de la metodología AIR al caso específico Peruano en materia de ciberincidentes, para la situación en la que nos encontramos consideramos que es favorable, esto debido a que si bien el Estado Peruanos se ha caracterizado por ser un Estado con controles de tipo ex – post, la materia analizado hace necesario que se implementen mecanismos de control ex – ante, este primer resultado, ordena la idea acerca de en qué momento se debería aplicar la herramienta legislativa, que en el presente caso tendría un carácter disuasivo en el tratamiento de cibercriminales.

La metodología aplicada al presente caso, nos permite, agrandar más la brecha existente entre conceptos que muchas veces utilizábamos como sinónimos, Informático y Cibernético, si bien en ambos caso se deberá contar con ambos tipos de control, es necesario saber que en materia informática la comisión del hecho se consuma con la obtención ilícita de la información, mientras que en materia cibernética la comisión del hecho se consuma con la vulneración o afectación a los mecanismos de seguridad de un sistema informático, a manera de ejemplo: el termino informático podría ser una casa y el termino cibernético las puertas, candados y seguros que podamos implementar a manera de seguridad, con lo cual para un derecho penal con controles de tipo ex – post, el control se dará una vez consumado el acto de

sustracción de algún artículo de la casa, mientras que por la vulneración a las puertas, candados o seguros en materia cibernéticamente se consumara con la sola violación a los mecanismos de seguridad, y el control de tipo ex – ante propone que la casa este continuamente vigilada por mecanismos alternativos como patrullaje o alarmas en los puntos de acceso.

Con este ejemplo creemos que la figura de los controles en materia informática y cibernética queda clara, es necesario que ambos se complementen de manera adecuada para así poder protegernos antes posibles ciberincidentes dentro del Ciber espacio.

4. Recomendaciones

Es necesaria la implementación de ambos tipos de controles, pues de otra forma la seguridad en materia informática y cibernética no se estaría ofreciendo de forma adecuada, y el Estado como garante de la Soberanía debe ser el principal actor dentro de esta lucha.

El Estado se encuentra en constante búsqueda de la represión de las actividades ilícitas, esto sin contar con las presiones internacionales que vienen por parte de países vecinos los cuales a través del ciberespacio pueden realizar una labor de espionaje con mucho mejor índice de anonimato, es por ellos que ambos tipos de controles son necesarios, por un lado para evitar posibles ataques probando las redes de forma constante, y por otro con un sistema represivo de conductas que sirva de disuasión en materia penal, asi como los mecanismos de colaboración internacional a los cuales el Perú debería de adherirse.

GLOSARIO DE TERMINOS

1. Attack – Ataque.

   An attack that alters a system or data - **Un ataque es algo que altera un sistema o los datos.**

   Fuente: Glossary of Key Information Security Terms, eds. Richard Kissel, National Institute for Standards and Technology, US Deparment of Commerce, NISTIR 7298, Revision 2 (2010)

   An attack on the authentication protocol where the Attacker transmits data to the Claimant, Credential Service Provider, Verifier, or Relying Party. Examples of active attacks include man-in-the-middle, impersonation, and session hijacking. - **Un ataque sobre el protocolo de autenticación en el que el atacante transmite datos a la Demandante, proveedor de servicios de credenciales, verificador, o de confianza. Ejemplos de ataques activos incluyen man-in-the-middle, la suplantación y el secuestro de sesión.**

   Fuente: Glossary of Key Information Security Terms, eds. Richard Kissel, National Institute for Standards and Technology, US Deparment of Commerce, NISTIR 7298, Revision 2 (2006)

   An actual assault perpetrated by an intentional threat source that attempts to alter a system, its resources, its data, or its operations. - **Un asalto real perpetrado por una fuente de amenaza intencional que intenta alterar un sistema, sus recursos, sus datos, o sus operaciones.**

   Fuente: Compilation of Existing Cybersecurity and Information Security Related Defintions, Open Technology Institute New America (2015 July)

2. Activities of the Armed Forces in information space - Actividades de las Fuerzas Armadas en el espacio de información

   Use by the Armed Forces of the information resources for solving the tasks of defence and security. - **El uso por las Fuerzas Armadas de los recursos de información para la solución de las tareas de defensa y seguridad.**

Fuente: Conceptual Views Regarding the Activiites of the Armed Forces of the Russian Federation in the Informaiton Space (2011)

3. Advanced Persistent Threat - Amenaza persistente avanzada.

   An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives. - **Un adversario que posee niveles sofisticados de experiencia y recursos significativos que le permitan crear oportunidades para lograr sus objetivos mediante el uso de múltiples vectores de ataque (por ejemplo, cibernética, física, y el engaño). Estos objetivos suelen incluir el establecimiento y ampliación de pie ejerce dentro de la infraestructura de tecnología de la información de las organizaciones dirigidas a los efectos de filtrar información, menoscabar o anular los aspectos críticos de una misión, programa u organización; o posicionándose para llevar a cabo estos objetivos en el futuro. La amenaza persistente avanzada: (i) persigue sus objetivos repetidamente durante un período prolongado de tiempo; (Ii) se adapta a los esfuerzos de los defensores de resistirse a ella; y (iii) se determina para mantener el nivel de interacción necesario para ejecutar sus objetivos.**
   Fuente: NIST US Department of Commerce: Glossary of Key Information Security Terms (June 2013)

   An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). - **Un adversario que posee niveles sofisticados de experiencia y recursos significativos que le permitan crear oportunidades para lograr sus objetivos mediante el uso de múltiples vectores de ataque (por ejemplo, cibernética, física, y el engaño).**
   Fuente: United States of America, Department of Homeland Security, National Initiative for Cybersecurity Careers and Studies, "Explore

Terms: A Glossary of Common Cybersecurity Terminology" ND. http://niccs.us-cert.gov/glossary

A group, such as a foreign government, with both the capability and intent to continually and effectively target a specific entity, often to conduct espionage or attack operations. - **Un grupo, como por ejemplo un gobierno extranjero, tanto con la capacidad y la intención de manera constante y eficaz objetivo a una entidad específica, a menudo para llevar a cabo operaciones de espionaje o de ataque.**
Fuente: United States of America, Democratic Policy & Communications Center, "Glossary of Cyber Related Terms"

4. Adversary – Adversario

   Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities. - **Individuo, grupo, organización o gobierno que lleva a cabo o tiene la intención de llevar a cabo actividades perjudiciales.**
   Fuente: Glossary of Key Information Security Terms, eds. Richard Kissel, National Institute for Standards and Technology, US Deparment of Commerce, NISTIR 7298, Revision 2 - 2012

5. Attacker – Atacante

   Any person deliberately exploiting vulnerabilities in technical and non-technical security controls in order to steal or compromise information systems and networks, or to compromise availability to legitimate users of information system and network resources. - **Cualquier persona que deliberadamente explotar vulnerabilidades en los controles técnicos y no técnicos de seguridad con el fin de robar o comprometer los sistemas y redes de información, y poner en peligro la disponibilidad para los usuarios legítimos del sistema de información y recursos de la red.**
   Fuente: Compilation of Existing Cybersecurity and Information Security Related Defintions, Open Technology Institute New America - 2005

   An individual, group, organization, or government that executes an attack. Extended Definition: A party acting with malicious intent to compromise an information system. - **Un individuo, grupo, organización o gobierno que ejecuta un ataque. Definición ampliada: Una parte que actúe con intenciones maliciosas para comprometer un sistema de información.**

Fuente: Compilation of Existing Cybersecurity and Information Security Related Defintions, Open Technology Institute New America - 2015 July

6. Close Action [Cyber] Operation – Operación cerca de Acción Cibernética

   A cyber operation requiring physical proximity to the targeted system. - **Una operación que requiere proximidad física cibernética con el sistema de destino.**
   Fuente: Tallinn Manual on the International Law Applicable to Cyber Warfare - 2013

7. Computer Network - Red de computadoras

   An Information Structure used to permit computers to exchange data. The infrastructure may be wired (e.g., Wi-Fi), or a combination of the two. - **Una estructura de información utilizada para permitir que los ordenadores intercambiar datos. La infraestructura puede ser cableada (por ejemplo, Wifi), o una combinación de los dos.**

   Fuente: Tallinn Manual on the International Law Applicable to Cyber Warfare - 2013

8. Computer Network Attack – Ataque de Red a un Ordenador.

   Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. - **Las medidas adoptadas a través del uso de redes de ordenadores para interrumpir, negar, degradar o destruir la información almacenada en los ordenadores y redes informáticas, o los ordenadores y las propias redes.**
   Fuente: Glossary of Key Information Security Terms, eds. Richard Kissel, National Institute for Standards and Technology, US Deparment of Commerce, NISTIR 7298, Revision 2 - 2010

   Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Also called CNA. - **Las medidas adoptadas a través del uso de redes de ordenadores para interrumpir, negar, degradar o destruir la información almacenada en los ordenadores y redes informáticas, o los ordenadores y las propias redes. También se llama la CNA.**

Fuente: Compilation of Existing Cybersecurity and Information Security Related Defintions, Open Technology Institute New America

Action taken to disrupt, deny, degrade or destroy information resident in a computer and/or computer network, or the computer and/or computer network itself. Note: A computer network attack is a type of cyber attack. - **Medidas adoptadas para interrumpir, negar, degradar o destruir la información almacenada en una computadora y / o red de computadoras, o la computadora y / o la propia red de ordenadores. Nota: Un ataque a la red informática es un tipo de ataque cibernético.**
Fuente: Compilation of Existing Cybersecurity and Information Security Related Defintions, Open Technology Institute New America - 2014

Activities that are conducted in and through the cyberspace in order to manipulate, obstruct, deny, downgrade or destroy information stored in the ICT networks or in the computer systems, or the ICT networks or in the computer systems themselves. **- Las actividades que se llevan a cabo en y por el ciberespacio con el fin de manipular, obstaculizar, negar, degradar o destruir la información almacenada en las redes de TIC o en los sistemas informáticos o las redes de TIC o en los sistemas informáticos propios.**

Fuente: Compilation of Existing Cybersecurity and Information Security Related Defintions, Open Technology Institute New America - 2013

9. Computer Network Defense – Red de Defensa de Ordenadores
Actions taken to defend against unauthorized activity within computer networks. CND includes monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities. - **Las medidas adoptadas para defenderse de la actividad no autorizada dentro de las redes de ordenadores. CDN incluye el monitoreo, detección, análisis (tales como análisis de tendencias y patrones), y la respuesta y la restauración de las actividades.**
Fuente: Glossary of Key Information Security Terms, eds. Richard Kissel, National Institute for Standards and Technology, US Deparment of Commerce, NISTIR 7298, Revision 2 - 2013

Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense information systems and computer networks. Also called CND. - **Las medidas adoptadas para proteger, controlar, analizar, detectar y responder a la actividad no autorizada dentro de los sistemas**

de información del Departamento de Defensa y las redes informáticas. También se llama CDN.
Fuente: National Initiative for Cybersecurity and Career and Studies, "Explore Terms: A Glossary of Common Cybersecurity Terminology", http://niccs.us-cert.gov/glossary - 2013

Actions taken by using computer networks for protecting, monitoring, analyzing, detecting, and hindering non-authorized activities carried out against computer networks and IT systems - **Las acciones tomadas por el uso de las redes de ordenadores para la protección, seguimiento, análisis, detección y obstaculizar las actividades no autorizadas llevadas a cabo contra las redes de ordenadores y sistemas informáticos.**
Fuente: Compilation of Existing Cybersecurity and Information Security Related Defintions, Open Technology Institute New America

10. Critical Cyber Infrastructure – Infraestructuras Criticas Cibernéticas
The cyber infrastructure that is essential to vital services for public safety, economic stability, national security, international stability and for the sustainability and restoration of critical cyberspace. - **La infraestructura cibernética que es esencial para los servicios vitales para la seguridad pública, la estabilidad económica, la seguridad nacional, la estabilidad internacional y para la sostenibilidad y la restauración del ciberespacio crítico.**

Fuente: East-West Institute, Critical Terminology Foundations 2, Russia-US Bilateral on Cybersecurity, Eds. Habes B. Godwin III, Andrey Kulpin, Kal Frederick Rauscher and Valery Yaschenko, Policy Report 2/2014, - 2014

11. Critical Cyber Services - Servicios críticos cibernéticos

Cyber services that are vital to preservation of public safety, economic stability, national security and international stability. - S**ervicios cibernéticos que son vitales para la preservación de la seguridad pública, la estabilidad económica, la seguridad nacional y la estabilidad internacionales.**
Fuente: East-West Institute, Critical Terminology Foundations 2, Russia-US Bilateral on Cybersecurity, Eds. Habes B. Godwin III, Andrey Kulpin, Kal Frederick Rauscher and Valery Yaschenko, Policy Report 2/2014, - 2014

12. Critical Cyberspace - El ciberespacio crítico

Cyber infrastructure and cyber services that are vital to preservation of public safety, economic stability, national security and international stability. - **Infraestructura y servicios Cibernéticos que son vitales para la preservación de la seguridad pública, la estabilidad económica, la seguridad nacional y la estabilidad internacionales.**
Fuente: East-West Institute, Critical Terminology Foundations 2, Russia-US Bilateral on Cybersecurity, Eds. Habes B. Godwin III, Andrey Kulpin, Kal Frederick Rauscher and Valery Yaschenko, Policy Report 2/2014, - 2014

13. Critical Information Infrastructure – Infraestructura de Información Critica

Critical information infrastructure (CII) may refer to any IT systems which support key assets and services within the national infrastructure. - **Infraestructura de información crítica (CII) puede referirse a un sistema de TI que soportan los bienes y servicios clave dentro de la infraestructura nacional.**
Fuente: Compilation of Existing Cybersecurity and Information Security Related Defintions, Open Technology Institute New America - 2011

The ITU regards Critical Information Infrastructure as the virtual element of critical infrastructure. The information and communicaiton tehcnologies, that from CII, increasingly operatie and control critical national sectors such as health, water, transport, communicaitons, governmetn, energy, food, finance and emergency services, their physical assets and the activities of personnel. - **La UIT se refiere a infraestructuras críticas de información como el elemento virtual de la infraestructura crítica. Las tecnologías de la información y de la comunicación, que a partir de la CII, cada vez operan y controlar sectores críticos nacionales como la salud, el agua, el transporte, comunicación, gobierno, energía, alimentos, finanzas y servicios de emergencia, sus activos físicos y las actividades del personal.**
Fuente: Computer Misuse Act - 2011

Critical information infrastructure shall mean an electronic communications network, information system or a group of information systems where an incident that occurs causes or may cause grave damage to national security, national economy or social well-being. - Infraestructura de información crítica se entenderá red y las comunicaciones electrónicas, sistemas de información o de un grupo de sistemas de información, donde se produce un incidente que

cause o pueda causar un grave daño a la seguridad nacional, la economía nacional o social, o el bienestar.
Fuente: Approval of the programme for the development of electronic information security (cyber-security) for 2011-2019 - 2010

Critical information infrastructure means an element or system of elements of the critical infrastructure in the sector of communication and information systems within the field of cybersecurity - **Infraestructura de información crítica, un elemento o sistema de elementos de la infraestructura crítica en el sector de los sistemas de comunicación e información en el ámbito de la seguridad cibernética.**
Fuente: Compilation of Existing Cybersecurity and Information Security Related Defintions, Open Technology Institute New America - 2015

Critical information infrastructure refers to the structures and functions behind the information systems of the vital functions of society which electronically transmit, transfer, receive, store or otherwise process information (data). - **Infraestructura de información crítica se refiere a las estructuras y funciones detrás de los sistemas de información de las funciones vitales de la sociedad que transmiten electrónicamente, transferir, recibir, almacenar o procesar información (datos).**
Fuente: Finland's Cyber Security Strategy - 2010

14. Critical Infrastructure - Infraestructura crítica

Physical or virtual systems and assets under the jurisdiction of a State that are so vital that their incapacitation or destruction may debilitate a State's security, economy, public health or safety, or the environment. - **Sistemas físicos o virtuales y activos bajo la jurisdicción de un Estado que son tan vitales que su incapacitación o destrucción pueden debilitar la seguridad, la economía, la salud de un Estado o la seguridad pública o el medio ambiente.**
Fuente: Tallinn Manual on the International Law Applicable to Cyber Warfare - 2013

Includes electronic information and communications systems and services and the information contained in these systems and services. Information and communications systems and services are composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all

other media types. Communications include sharing and distribution of information. For example: computer systems; control systems (e.g., supervisory control and data acquisition–SCADA); networks, such as the Internet; and cyber services (e.g., managed security services) are part of cyber infrastructure. - **Incluye los sistemas y servicios de información electrónicos y de las comunicaciones y la información contenida en estos sistemas y servicios. Sistemas y servicios de información y comunicación están compuestos hardware y software que procesan, almacenan y transmiten información, o cualquier combinación de todos estos elementos. El procesamiento incluye la creación, acceso, modificación y destrucción de la información. Almacenamiento incluye papel, magnético, electrónico, y todos los otros tipos de medios. Comunicaciones incluyen el intercambio y la distribución de la información. Por ejemplo: sistemas informáticos; sistemas de control (por ejemplo, control de supervisión y adquisición de datos SCADA); redes, como Internet; y los servicios cibernéticos (por ejemplo, los servicios de seguridad gestionada) son parte de la infraestructura cibernética.**
Fuente: NIST US Department of Commerce: Glossary of Key Information Security Terms (June 2013)

Although governments administer only a minority of the Nation`s critical infrastructure computer systems, governments at all levels perform essential services that rely on each of the critical infrastructure sectors, which are agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping. - **A pesar de que los gobiernos administran sólo una minoría de los sistemas informáticos de infraestructura crítica de la nación, los gobiernos en todos los niveles de desempeño de los servicios esenciales dependen de cada uno de los sectores de infraestructuras críticas, que son: la agricultura, la alimentación, el agua, la salud pública, servicios de emergencia, el gobierno, la base industrial de defensa , la información y las telecomunicaciones, la energía, el transporte, la banca y las finanzas, productos químicos y materiales peligrosos, y postal y envío.**
Fuente: Compilation of Existing Cybersecurity and Information Security Related Defintions, Open Technology Institute New America - 2003

System and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would

have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. [Critical Infrastructures Protection Act of 2001, 42 U.S.C. 5195c(e)]. - **Sistema y activos, ya sea físico o virtual, tan vital para los EE.UU. que la incapacidad o destrucción de dichos sistemas y activos tendrían un efecto debilitante sobre la seguridad, la seguridad económica nacional, la salud pública o la seguridad nacional, o cualquier combinación de estos asuntos. [Ley de protección de infraestructuras críticas de 2001, 42 USC 5195c (e)].**
Fuente: Glossary of Key Information Security Terms, eds. Richard Kissel, National Institute for Standards and Technology, US Deparment of Commerce, NISTIR 7298, Revision 2, - 2013

Information infrastructure is a key component of Canada`s critical infrastructure, which includes the following sectors: energy and utilities, communications and information technology, finance, health care, food, water, transportation, Government and manufacturing. The challenges of securing the information infrastructure are the same across all sectors, of which up to 90 per cent is estimated to be owned and operated privately. - **Infraestructura de la información es un componente clave de la infraestructura crítica de Canadá, que incluye los siguientes sectores: energía y servicios públicos, comunicaciones y tecnología de la información, finanzas, cuidado de la salud, alimentos, agua, transporte, gobierno y fabricación. Los desafíos de asegurar la infraestructura de información son los mismos en todos los sectores, de los cuales se estima que es de propiedad hasta un 90 por ciento y de gestión privada.**
Fuente: Compilation of Existing Cybersecurity and Information Security Related Defintions, Open Technology Institute New America - 2005

Critical infrastructure refers to infrastructure whose disruption, failure or destruction would have serious implications for society, the private sector and the state. It includes, for example, control and switchgear for energy supply or telecommunications. An inventory of critical infrastructure will be compiled by the national strategy for the protection of critical infrastructure. - **Infraestructura crítica se refiere a la infraestructura cuya interrupción, insuficiencia o destrucción tendría graves consecuencias para la sociedad, el sector privado y el Estado. Incluye, por ejemplo, el control y maniobra para el suministro de energía o las telecomunicaciones. Un inventario de la infraestructura crítica será compilada por la estrategia nacional para la protección de infraestructuras críticas.**

Fuente: Compilation of Existing Cybersecurity and Information Security Related Defintions, Open Technology Institute New America - 2012

Critical infrastructures are formed by business entities providing highly irreplaceable services and are essential for people`s social lives and economic activities. If its function is suspended, reduced or unavailable, peoples social lives and economic activities will be greatly disrupted, and the same below. - **Las infraestructuras críticas son formados por las entidades empresariales que prestan servicios altamente irreemplazables y son esenciales para la vida social de la gente y las actividades económicas. Si se suspende su función, reducida o no disponibles, los pueblos la vida social y las actividades económicas se verá afectadas en gran medida, y lo mismo más adelante.**
Fuente: Compilation of Existing Cybersecurity and Information Security Related Defintions, Open Technology Institute New America - 2006

Critical infrastructures are organizations or institutions with major importance for the public good, whose failure or damage would lead to sustainable supply bottlenecks, considerable disturbance of public security or other dramatic consequences. At federal level, the following areas have been identified: Energy, information technology and telecommunication, transport, health, wather, food, finance and insurance sector, state and administration, media and culture. - **Las infraestructuras críticas son las organizaciones o instituciones con mayor importancia para el bien público, cuyo fallo o daño daría lugar a problemas de abastecimiento sostenibles, una considerable perturbación de la seguridad pública u otras consecuencias dramáticas. A nivel federal, se han identificado las siguientes áreas: energía, tecnología de la información y de las telecomunicaciones, el transporte, la salud, vigilante, la comida, las finanzas y el sector de los seguros, el estado y la administración, medios de comunicación y la cultura.**
Fuente: Compilation of Existing Cybersecurity and Information Security Related Defintions, Open Technology Institute New America - 2011

Critical infrastructure is defined as those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would adversely impact on the social or economic well-being of the nation or affect Australia´s ability to ensure national security. - I**nfraestructura crítica se define como aquellas instalaciones físicas, cadenas de suministro, tecnologías de la información y redes de comunicación que, de ser destruido, degradado o indisponible durante un período prolongado, podría tener**

efectos nocivos para el bienestar social o económico de la nación o afectar la capacidad de Australia para garantizar la seguridad nacional.
Fuente: Compilation of Existing Cybersecurity and Information Security Related Defintions, Open Technology Institute New America - 2013

15. Critical Infrastructure Protection - Protección de infraestructuras críticas

Actions taken to prevent, remediate, or mitigate the risks resulting from vulnerabilities of critical infrastructure assets. Also called CIP. See also defense critical infrastructure. - **Las medidas tomadas para prevenir, remediar o mitigar los riesgos derivados de las vulnerabilidades de los activos de infraestructura crítica. También se llama CIP. Ver también la infraestructura crítica de defensa.**

Fuente: US Department of Defense Dictionary of Military and Assosicated Terms

16. Cyber – Ciber

The word 'cyber' is almost invariably the prefix for a term or the modifier of a compound word, rather than a stand-alone word. Its inference usually relates to electronic information (data) processing, information technology, electronic communications (data transfer) or information and computer systems. Only the complete term of the compound word (modifier+head) itself can be considered to possess actual meaning. The word cyber is generally believed to originate from the Ancient Greek verb κυβερεω (kybereo) "to steer, to guide, to control". - **La palabra 'cibernética' es casi siempre el prefijo para un término o el modificador de la palabra compuesta, en lugar de una palabra independiente. Su deducción por lo general se refiere a la información electrónica de procesamiento (datos), tecnología de la información, las comunicaciones electrónicas (transferencia de datos) o los sistemas de información y computación. Sólo el término completo de la palabra compuesto (modificador + cabeza) en sí se puede considerar que posee significado real. La palabra cibernética en general se cree que proceden de la antigua κυβερεω verbo griego (kybereo) "para dirigir, guiar, controlar". Fuente:**
Fuente: Finland's Cyber Security Strategy Government Resolution 24 Jan 2013

Relating to or characteristic of the culture of computers, information technology, and virtual reality. - **En relación con o característica de la cultura de la informática, tecnología de la información, y la realidad virtual.**
Fuente: Oxford Dictionary

Connotes a relationship with information technology. - **Connota una relación con la tecnología de la información.**
Fuente: Tallinn Manual on the International Law Applicable to Cyber Warfare - 2013

Anything relating to, or involving, computers or computer networks (such as Internet). - todo lo relacionado con, o que involucren a ordenadores o redes de ordenadores (como Internet).
Fuente: Strategy on Cyber Security of Montenegro to 2017 (2013)

17. Cyber Attack – Ciber Ataque

The term "cyber attack" refers to an attack through IT in cyber space, which is directed against one or several IT system(s). Its aim is to undermine the objectives of ICT security protection (confidentiality, integrity and availability) partly or totally. - **El término "ataque cibernético" se refiere a un ataque a través de él en el espacio cibernético, que está dirigido contra uno o varios de sistema (s) de TI. Su objetivo es socavar los objetivos de protección de la seguridad TIC (confidencialidad, integridad y disponibilidad) en parte o totalmente.**
Fuente: Austrian Cyber Security Strategy (2013)

Cyber attacks include the unintentional or unauthorised access, use, manipulation, interruption or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information. The severity of the cyber attack determines the appropriate level of response and/or mitigation measures: i.e., cyber security. - **Los ataques cibernéticos incluyen el acceso involuntario o no autorizado, uso, manipulación, interrupción o destrucción (a través de medios electrónicos) de información electrónica y / o la infraestructura física y electrónica utilizada para procesar, comunicar y / o almacenar esa información. La gravedad del ataque cibernético determina el nivel apropiado de respuesta y / o medidas de mitigación: es decir, la seguridad cibernética.**
Fuente: Canada's Cyber Security Strategy (2010)

A cyber attack is an IT attack in cyberspace directed against one or several other IT systems and aimed at damaging IT security. The aims of IT security, confidentiality, integrity and availability may all or individually be compromised. Cyber attacks directed against the confidentiality of an IT system, which are launched or managed by foreign intelligence services, are called cyber espionage. Cyber attacks against the integrity and availability of IT systems are termed cyber sabotage. - **Un ataque cibernético es un ataque de TI en el ciberespacio dirigido contra uno o varios otros sistemas de TI y dirigido a la seguridad informática dañina. Los objetivos de la seguridad informática, la confidencialidad, la integridad y la disponibilidad pueden ser todos o individualmente verse comprometidas. Los ataques cibernéticos dirigidos contra la confidencialidad de un sistema informático, que son lanzados o gestionados por los servicios de inteligencia extranjeros, se llaman espionaje cibernético. Ataques cibernéticos contra la integridad y disponibilidad de los sistemas informáticos se denominan sabotaje cibernético.**

Fuente: Cyber Security Strategy for Germany (2011)

Action taken to disrupt, deny, degrade or destroy information resident in a computer and/or computer network, or the computer and/or computer network itself. Note: A computer network attack is a type of cyber attack. - **Medidas adoptadas para interrumpir, negar, degradar o destruir la información almacenada en una computadora y / o red de computadoras, o la computadora y / o la propia red de ordenadores. Nota: Un ataque a la red informática es un tipo de ataque cibernético.**
Fuente: NATO AAP-06 Edition 2014

[Cyberattack] An attempt by hackers to damage or destroy a computer network or system. - **[Ataque cibernético] Un intento por los hackers para dañar o destruir una red o sistema informático.**

Fuente: Oxford Dictionary

An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. - **Un ataque, a través del ciberespacio, la orientación uso de una empresa del ciberespacio con el propósito de interrumpir, desactivar, destruir o controlar malintencionadamente un entorno**

informático / infraestructura; o destruir la integridad de los datos o el robo de información controlada.
Fuente: CNSS Instruction No. 4009 (26 Apr 2010)

A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.- **Un ataque cibernético es una operación cibernética, ya sea ofensiva o defensiva, que se espera razonablemente causar lesiones o la muerte a personas o daños o destrucción de objetos.**
Fuente: Tallinn Manual on the International Law Applicable to Cyber Warfare – 2013, Rule 30

18. Cyber Crime – Ciber Crimen

The Australian Government defines cyber crime as those computer offences under the Commonwealth Criminal Code Act 1995 (Part 10.7) which involve the unauthorised access to, modification or impairment of electronic communications. - **El Gobierno de Australia define los delitos cibernéticos como los delitos informáticos en virtud de la Ley de Código Penal de la Commonwealth de 1995 (Parte 10.7) que implican el acceso no autorizado a, modificación o alteración de las comunicaciones electrónicas.**
Fuente: Australian Government, Cyber Security Strategy (2009)

Cyber crime comprises illegal attacks from cyber space on or through ICT systems, which are defined in penal or administrative laws. The term therefore covers all criminal offences committed with the aid of information technologies and communications networks and also encompasses Internet crime. - **La ciberdelincuencia comprende ataques ilegales desde el espacio cibernético en oa través de los sistemas de TIC, que se definen en las leyes penales o administrativas. Por tanto, el término abarca todos los delitos cometidos con la ayuda de tecnologías de la información y las redes de comunicación y también abarca la delincuencia en Internet.**
Fuente: Austrian Cyber Security Strategy (2013)

Acts contravening international treaties and national laws, targeting networks or information systems, or using them to commit an offence or crime. – **Hechos que contravienen los tratados internacionales y las leyes nacionales, dirigidos a las redes y sistemas de información, o utilizarlos para cometer un delito o crimen**.
Fuente: Information Systems and Defence – France's Strategy (2011)

Any crime where information and communications technology is:
1. used as a tool in the commission of an offence
2. the target of an offence
3. a storage device in the commission of an offence.
In New Zealand some of the most common examples of cyber crime include fraud, identity theft and organised crime. - **Cualquier crimen donde la tecnología de la información y las comunicaciones son:**
1. utilizado como una herramienta en la comisión de un delito
2. el blanco de un delito
3. Un dispositivo de almacenamiento en la comisión de un delito.
En Nueva Zelanda algunos de los ejemplos más comunes de la delincuencia cibernética incluyen fraude, robo de identidad y el crimen organizado.
Fuente: New Zealand's Cyber Security Strategy (June 2011)

[Cybercrime] Crime conducted via the Internet or some other computer network. - **[Cibercrimen] Delito llevó a cabo a través de Internet o cualquier otra red informática.**
Fuente: Oxford Dictionary

The use of cyberspace for criminal purposes as defined by national or international law. - **El uso del ciberespacio para fines delictivos según lo definido por la legislación nacional o internacional.**
Fuente: East-West Institute, Critical Terminology Foundations 2, Russia-US Bilateral on Cybersecurity, Eds. Habes B. Godwin III, Andrey Kulpin, Kal Frederick Rauscher and Valery Yaschenko, Policy Report 2/2014, - 2014

19. Cyber Defense – Ciber Defensa
The term "cyber defence" refers to all measures to defend cyber space with military and appropriate means for achieving military-strategic goals. Cyber defence is an integrated system, comprising the implementation of all measures relating to ICT and information security, the capabilities of milCERT and CNO (Computer Network Operations) as well as the support of the physical capabilities of the army. - **El término "ciberdefensa" se refiere a todas las medidas para defender el espacio cibernético con medios militares y adecuados para alcanzar los objetivos estratégicos militares. Ciberdefensa es un sistema integrado, que comprende la aplicación de todas las medidas relacionadas con la seguridad de las TIC y la información, las capacidades de milCERT y CNO**

(Operaciones de la Red de ordenadores), así como el apoyo de las capacidades físicas del ejército.
Fuente: Austrian Cyber Security Strategy (2013)

The set of all technical and non-technical measures allowing a State to defend in cyberspace information systems that it considers to be critical. - **El conjunto de todas las medidas técnicas y no técnicas que permiten a un Estado defenderse en los sistemas de información del ciberespacio que considera a ser crítico.**
Fuente: Information Systems and Defence – France's Strategy (2011)

Cyber defence is mainly used in military context, but it may be also related to criminal and espionage activities. NATO uses the following definition when referring to cyber defence the ability to safeguard the delivery and management of services in an operational Communications and Information Systems (CIS) in response to potential and imminent as well as actual malicious actions that originate in cyberspace. - C**iberdefensa se utiliza principalmente en el contexto militar, pero puede ser también relacionada con actividades criminales y de espionaje. La OTAN utiliza la siguiente definición al referirse a la ciberdefensa la capacidad de salvaguardar la prestación y gestión de servicios en una red de comunicaciones operativas y Sistemas de Información (CEI) en respuestas potenciales e inminentes, así como acciones maliciosas reales que se originaron en el ciberespacio.**
Fuente: Strategy on Cyber Security of Montenegro to 2017 (2013)

20. Cyber Defensive Capability – Capacidad de Ciber Defensa

Capability to effectively protect and repel against a cyber exploitation or cyber attack that may be used as a cyber deterrent. - **Capacidad para proteger y repeler contra una explotación cibernética o ataque cibernético que puede ser utilizado como una disuasión cibernética eficazmente**
Fuente: East-West Institute, Critical Terminology Foundations 2, Russia-US Bilateral on Cybersecurity, Eds. Habes B. Godwin III, Andrey Kulpin, Kal Frederick Rauscher and Valery Yaschenko, Policy Report 2/2014, - 2014

21. Cyber Emergency – Ciber Emergencia

State of cyber emergency means a state, during which information security in information systems or services or electronic communication networks security is seriously endangered and the interests of the Czech Republic may thus be violated or

endangered. - **Estado de emergencia cibernética significa un estado, durante el cual la información de seguridad en sistemas de información o servicios o redes de comunicaciones electrónicas seguridad se pone en peligro de extinción y los intereses de la República Checa por lo tanto pueden ser violados o en peligro.**
Fuente: Czech Republic Draft Act on Cyber Security (2014)

22. Cyber Entity – Entidad Cibernética

Any distinct thing or actor that exists within the cyber infrastructure. - **Cualquier cosa distinta o actor que existe dentro de la infraestructura cibernética.**

Fuente: East-West Institute, Critical Terminology Foundations 2, Russia-US Bilateral on Cybersecurity, Eds. Habes B. Godwin III, Andrey Kulpin, Kal Frederick Rauscher and Valery Yaschenko, Policy Report 2/2014

23. Cyber Environment – Medio Ambiente Cibernético

This includes users, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks. - **Esto incluye a los usuarios, redes, dispositivos, todo el software, los procesos, la información en el almacenamiento o el transporte, aplicaciones, servicios y sistemas que se pueden conectar directa o indirectamente a las redes.**
Fuente: ITU Publications X.1205 : Overview of cybersecurity (2008)

24. Cyber Espionage – Ciber Espionaje

Cyber attacks directed against the confidentiality of an IT system are referred to as "cyber espionage", i.e. digital spying. Cyber attacks directed against the integrity and availability of an IT system are referred to as cyber sabotage. - **Los ataques cibernéticos dirigidos contra la confidencialidad de un sistema de TI se les conoce como "espionaje cibernético", es decir, el espionaje digital. Los ataques cibernéticos dirigidos contra la integridad y la disponibilidad de un sistema de TI se denominan como el sabotaje cibernético.**
Fuente: Austrian Cyber Security Strategy (2013)

A cyber attack is an IT attack in cyberspace directed against one or several other IT systems and aimed at damaging IT security. The aims

of IT security, confidentiality, integrity and availability may all or individually be compromised. Cyber attacks directed against the confidentiality of an IT system, which are launched. Or managed by foreign intelligence services, are called cyber espionage. Cyber attacks against the integrity and availability of IT systems are termed cyber sabotage. - **Un ataque cibernético es un ataque de TI en el ciberespacio dirigido contra uno o varios otros sistemas de TI y dirigido a la seguridad informática dañina. Los objetivos de la seguridad informática, la confidencialidad, la integridad y la disponibilidad pueden ser todos o individualmente verse comprometidas. Los ataques cibernéticos dirigidos contra la confidencialidad de un sistema informático, que se puso en marcha. O gestionados por los servicios de inteligencia extranjeros, están llamados espionaje cibernético. Ataques cibernéticos contra la integridad y disponibilidad de los sistemas informáticos se denominan sabotaje cibernético.**
Fuente: Cyber Security Strategy for Germany (2011)

[Cyberespionage] The use of computer networks to gain illicit access to confidential information, typically that held by a government or other organization. - **[Espionaje cibernético] El uso de las redes de ordenadores para obtener acceso ilícito a la información confidencial, por lo general en manos de un gobierno u otra organización.**

Fuente: Oxford Dictionary

Defined narrowly as any act undertaken clandestinely or under false pretences that uses cyber capabilities to gather (or attempt to gather information with the intention of communicating it to the opposing party. The act must occur in a territory controlled by a party to the conflict. - **Estrechamente definido como cualquier acto llevado a cabo clandestinamente o con falsos pretextos que utiliza capacidades cibernéticas para recoger (o intentar recopilar información con la intención de comunicar a la parte contraria. El acto debe producirse en un territorio controlado por una parte en el conflicto.**
Fuente: Tallinn Manual on the International Law Applicable to Cyber Warfare – 2013, Rule 66

A cyber operation to obtain unauthorized access to sensitive information throguh covert means. - **Una operación cibernética para obtener acceso no autorizado a información sensible a través de medios encubiertos.**

Fuente: East-West Institute, Critical Terminology Foundations 2, Russia-US Bilateral on Cybersecurity, Eds. Habes B. Godwin III, Andrey Kulpin, Kal Frederick Rauscher and Valery Yaschenko, Policy Report 2/2014, - 2014

Cyber attacks have aimed to steal sensitive information and data from financial, government and utilities infrastructure targets. These attacks can target intellectual property or sensitive information about organisations or government. - **Los ataques cibernéticos destinados a robar información confidencial y los datos de objetivos de la infraestructura financiera, gobierno y servicios públicos. Estos ataques pueden dirigirse a la propiedad intelectual o información sensible acerca de las organizaciones o el gobierno.**
Fuente: Compilation of Existing Cybersecurity and Information Security Related Defintions, Open Technology Institute New America - 2011

Cyber espionage is defined narrowly as any act undertaken clandestinely or under false pretences that uses cyber capabilities to gather (or attempt to gather_ information with the intention of communicating it to the opposing party. The act must occur in territory controlled by a party to the conflict. - **El ciberespionaje se define estrictamente como cualquier acto llevado a cabo clandestinamente o con falsos pretextos que utiliza capacidades cibernéticas para recoger o intentar recopilar información con la intención de comunicar a la parte contraria. El acto debe producirse en el territorio controlado por una parte en el conflicto.**
Fuente: NATO CCD COE

25. Cyber Infrastructure – Ciber Infraestructura

Includes electronic information and communications systems and services and the information contained in these systems and services. Information and communications systems and services are composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications include sharing and distribution of information. For example: computer systems; control systems (e.g., supervisory control and data acquisition–SCADA); networks, such as the Internet; and cyber services (e.g., managed security services) are part of cyber infrastructure. **Incluye los sistemas y servicios de información electrónica y de las comunicaciones y la**

información contenida en estos sistemas y servicios. sistemas y servicios de información y comunicación están compuestas de todo el hardware y software que procesar, almacenar y transmitir información, o cualquier combinación de todos estos elementos. El procesamiento incluye la creación, acceso, modificación y destrucción de la información. Almacenamiento incluye papel, magnético, electrónico, y todos los otros tipos de medios. Comunicaciones incluyen el intercambio y la distribución de la información. Por ejemplo: sistemas informáticos; sistemas de control (por ejemplo, control de supervisión y adquisición de datos SCADA); redes, como Internet; y los servicios cibernéticos (por ejemplo, los servicios de seguridad gestionada) son parte de la infraestructura cibernética.
Fuente: Glossary of Key Information Security Terms, eds. Richard Kissel, National Institute for Standards and Technology, US Deparment of Commerce, NISTIR 7298, Revision 2, - 2010

26. Cyber Intelligence – Ciber Inteligencia

Activities using all "intelligence" sources in support of Cyber Security to map out the general cyber threat, to collect cyber intentions and possibilities of potential adversaries, to analyse and communicate, and to identify, locate, and allocate the source of cyber-attacks.
Actividades utilizando todas las fuentes de "inteligencia" en apoyo de Seguridad Cibernética para trazar la amenaza general cibernética, para recoger las intenciones cibernéticos y posibilidades de adversarios potenciales, analizar y comunicar, y para identificar, localizar y asignar el origen de los ataques cibernéticos.
Fuente: Compilation of Existing Cybersecurity and Information Security Related Defintions, Open Technology Institute New America - 2014

27. Cyber Offensive Capability – Capacidad de Ciber Ofensiva

A capabiltiy to initiate a cyber attackthat may be used as a cyber deterrent. **Una capacidad de iniciar un ataque cibernético que puede ser utilizado como un elemento disuasorio cibernético**
Fuente: East-West Institute, Critical Terminology Foundations 2, Russia-US Bilateral on Cybersecurity, Eds. Habes B. Godwin III, Andrey Kulpin, Kal Frederick Rauscher and Valery Yaschenko, Policy Report 2/2014, - 2014

28. Cyber Operations – Ciber Operación

> The employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace. **El empleo de las capacidades cibernéticas con el propósito principal de lograr los objetivos en o por el uso del ciberespacio.**

Fuente: Tallinn Manual on the International Law Applicable to Cyber Warfare - 2013