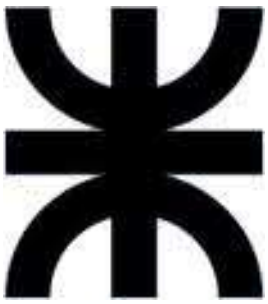

ESTRATEGIAS NACIONALES DE CIBERSEGURIDAD: ESTUDIO COMPARATIVO BASADO EN UN ENFOQUE TOP-DOWN DESDE UNA VISIÓN GLOBAL A UNA VISIÓN LOCAL

Alumno

Licenciado Eduardo LEIVA

Director: Mg. Hernán AMATRIAIN (UNLa)

TRABAJO PRESENTADO PARA OBTENER EL GRADO
DE
ESPECIALISTA EN INGENIERIA EN SISTEMAS DE INFORMACIÓN

ESCUELA DE POSGRADOS

FACULTAD REGIONAL BUENOS AIRES

UNIVERSIDAD TECNOLOGICA NACIONAL

NOVIEMBRE, 2015

Contenido

RESUMEN

El uso de las Tecnologías de Información y de Comunicación se ha incorporado de forma general a la vida cotidiana de una nación. Este nuevo escenario facilita un desarrollo sin precedentes en el intercambio de información y comunicaciones, pero al mismo tiempo conlleva serios riesgos y amenazas que pueden afectar a la Seguridad Nacional.

Varios son los factores que contribuyen a la proliferación de acciones delictivas en el ciberespacio, la rentabilidad que ofrece su explotación en términos económicos, políticos o de otro tipo, la facilidad y el bajo costo de las herramientas utilizadas para la consecución de ataques y la facilidad de ocultación del atacante, hacen posible que estas actividades se lleven a cabo de forma anónima, desde cualquier lugar del mundo y con impunidad. Esto tiene impacto sobre las distintas organizaciones en los sectores público y privado, y los propios ciudadanos. Los distintos perfiles de atacantes explotan las vulnerabilidades tecnológicas con el objeto de recabar información de valor para cometer ilícitos, como así también para amenazar los servicios básicos que pueden afectar al normal funcionamiento de un país.

La importancia estratégica de disponer de un ciberespacio seguro, conlleva la creación de un sistema de Ciberseguridad Nacional basado en una Estrategia Nacional de Ciberseguridad (ENCS), es decir, un conjunto de órganos, organismos y procedimientos que permitan la dirección, control y gestión de la seguridad en el ciberespacio.

Planteando la necesidad de una (ENCS), se puede observar que existen naciones que no poseen una estrategia de Ciberseguridad y otras que están en el proceso de elaboración de la misma. Advirtiendo la importancia de la situación, este trabajo tiene el propósito de realizar un estudio comparativo de algunas Estrategias Nacionales de Ciberseguridad seleccionadas y además brindar una visión general de la situación actual de la Argentina. El estudio se basa en el análisis de las estrategias publicadas por los países más avanzados en el tema, evaluando ventajas y desventajas y realizando una recopilación de recomendaciones y mejores prácticas.

ABSTRACT

The use of Information Technology and Communication is incorporated generally to the daily life of a nation. This new scenario provides an unprecedented development in the exchange of information and communications, but also has serious risks and threats that may affect national security.

There are several factors that contribute to the proliferation of criminal activities in cyberspace, the profitability offered their exploitation in economic, political or other terms, the ease and low cost of the tools used to achieve attacks and ease Hiding the attacker, enable these activities are carried out anonymously, from anywhere in the world with impunity. This has an impact on the various organizations in the public and private sectors, and the citizens themselves. The different profiles of attackers exploit technological vulnerabilities in order to obtain valuable information to commit crimes, as well as to threaten the basic services that may affect the normal functioning of a country.

The strategic importance of a secure cyberspace, involves the creation of a system of National Cybersecurity based on a National Cyber Security Strategy (NCSS), ie, a set of organs, agencies and procedures for the management, control and management security in cyberspace.

Raising the need for a (NCSS), you can see that there are nations that do not have a strategy for cybersecurity and others are in the process of preparing the same. Noting the importance of the situation, this paper aims to conduct a comparative study of some selected National Cyber Security Strategies and also provide an overview of the current situation of Argentina. The study is based on analysis of strategies published by the most advanced countries in the area, assessing advantages and disadvantages and making a list of recommendations and best practices.

1. INTRODUCCIÓN

En este Capítulo se plantea el contexto del trabajo (sección 1.1), se establece su objetivo (sección 1.2) y se describe su estructura (sección 1.3).

1.1. CONTEXTO DEL TRABAJO

En las últimas décadas, las nuevas tecnologías, los servicios electrónicos y redes de comunicación se han visto cada vez más integradas en nuestra vida diaria. Las empresas, la sociedad, el gobierno y la defensa nacional dependen del funcionamiento de las tecnologías de la información y comunicaciones (TICs) y de la operación de las Infraestructuras Críticas de Información (ICIs). El transporte, las comunicaciones, el comercio electrónico, los servicios financieros, los servicios de emergencia y servicios públicos se sustentan en la disponibilidad, integridad y confidencialidad de la información que fluye a través de estas infraestructuras.

Todo esto ha generado un nuevo escenario donde se puede apreciar la dependencia de las sociedades modernas y de los países desarrollados de los sistemas de información, lo que constituye la gran fortaleza de los mismos, como así también su gran debilidad. A pesar de los riesgos que conlleva una sociedad cada vez más interconectada, esta tendencia es imparable, lo que significa que hay que afrontar el futuro y gestionar los riesgos que arribarán. El contexto es variado, se puede observar una mayor y más compleja actividad criminal desarrollada por grupos organizados y por delincuentes individuales, una mayor y más compleja actividad de espionaje ya sea industrial, militar o política, una mayor variedad y cantidad de ataques a las infraestructuras críticas de las naciones, a las libertades públicas y a todo tipo de servicios en los que se basa el funcionamiento de las sociedades. Del mismo modo se puede apreciar un mayor índice de ataques enmascarados, dirigidos por Estados y encubiertos bajo la apariencia de ataques de bandas criminales, activistas políticos, hackers y otro tipo de atacantes. Como dato no menor se puede observar una mayor participación de individuos en acciones maliciosas, ya sea por ignorancia, por curiosidad, por diversión, por reto o por lucro. Cabe destacar, que la gran cantidad de riesgos surgen a causa de la atracción que el ciberespacio produce, al ofrecer una mayor rentabilidad, facilidad e impunidad para todo este tipo de actividades.

Entonces se puede decir que en la medida que la sociedad se vuelve más y más dependiente de las TICs, la protección y la disponibilidad de estos activos críticos, se convierte cada vez más en un

tema de interés nacional. Los incidentes que causan la interrupción de las infraestructuras críticas y los servicios de TICs podrían causar importantes impactos negativos en el funcionamiento de la sociedad y la economía. Como tal, el ciberespacio seguro se ha convertido en uno de los retos más importantes del siglo, y por lo tanto la seguridad informática se considera cada vez más como una cuestión nacional a nivel estratégico que afecta a todos los niveles de la sociedad.

Como reacción a esta avalancha de amenazas, que en definitiva se consideran amenazas al bienestar y al sistema democrático de los países, surge la necesidad de disponer de herramientas en defensa de sus legítimos intereses, esto implica el desarrollo de capacidades y habilidades en la prevención, defensa, detección, análisis, investigación, recuperación y respuesta a las amenazas, como así también la gestión de los riesgos asociados.

Una Estrategia Nacional de Ciberseguridad se puede considerar como un elemento fundamental en la ciberseguridad de una nación, que puede ayudar a mejorar la resistencia de las infraestructuras y servicios nacionales de información. Una estrategia se establece a un alto nivel en la estructura jerárquica de una nación, que establece una serie de objetivos nacionales y prioridades que deben alcanzarse en un plazo determinado. Como tal, proporciona un marco estratégico para los esfuerzos de una nación el plano de la ciberseguridad.

1.2. OBJETIVO DEL TRABAJO

En base a la problemática mencionada anteriormente y debido que existen naciones sobre todo en Latinoamérica, que no tienen desarrolladas sus estrategias, o que están trabajando en ella, en este trabajo se propone un Estudio Comparativo de las Estrategias Nacionales de Ciberseguridad de algunas naciones seleccionadas, basado en el análisis de ventajas y desventajas, recomendaciones y mejores prácticas sobre cómo desarrollar, implementar y mantener una estrategia de ciberseguridad.

Más específicamente, se pretende:

- Ayudar a definir las áreas de interés de una Estrategia Nacional de Ciberseguridad.
- Identificar mejores prácticas y recomendaciones útiles.
- Contribuir en el desarrollo, evaluación y actualización de una Estrategia Nacional de Ciberseguridad.

1.3. ESTRUCTURA DEL TRABAJO

En el Capítulo Introducción se plantea el contexto del trabajo, se establece su objetivo y se presenta una breve descripción de la estructura del mismo.

En el Capítulo Estado de la Cuestión se describe la Ciberdefensa y la Ciberseguridad, su situación actual. Se presentan algunas ENCS de países avanzados en el tema, se describe a cada una de ellas y se realiza una comparación analizando sus puntos claves. Del mismo modo se presentan algunas Políticas de Ciberseguridad de países Latinoamericanos, se describe a cada una de ellas y se realiza una comparación analizando sus puntos claves. Para finalizar este capítulo se presenta La Ciberseguridad Argentina, se presenta la situación actual y se muestran algunas vulnerabilidades reportadas en sitios gubernamentales.

En el Capítulo Posibles Cursos de Acción, se identifican los factores que aumentan los riesgos del ciberespacio, se identifican las áreas de vacancia donde se podría enfocar el trabajo y finalmente se realiza la identificación del problema de investigación.

2. ESTADO DE LA CUESTIÓN

En este capítulo se presenta el estado de la cuestión sobre distintas teorías y técnicas que son concurrentes con los objetivos de este trabajo. Se presenta la Ciberdefensa: situación actual (sección 2.1), la Ciberseguridad (sección 2.2), la Estrategia Nacional de Ciberseguridad (sección 2.3) y la Ciberseguridad Nacional Argentina (sección 2.4).

2.1. CIBERDEFENSA: SITUACIÓN ACTUAL

En la actualidad se puede observar que cuanto mayor es el índice de desarrollo de una sociedad, mayor dependencia se tiene de los sistemas de información y de las comunicaciones. Cualquier intrusión, manipulación, sabotaje o interrupción de dichos sistemas y de las ICIs pueden llegar a ser sufridos por millones de personas.

En los conflictos tradicionales existen fronteras y límites, mientras que en el ciberespacio no. Para realizar un ataque no es necesario desplazarse, moverse o tener que pasar una frontera, este es una de las principales características de este tipo de fenómeno. El ciberespacio es un ambiente único, sin fronteras geográficas, anónimo, asimétrico y puede ser considerado fácilmente clandestino.

Se define a la Ciberdefensa como la aplicación de medidas de seguridad para proteger las infraestructuras de los sistemas de información y comunicaciones frente a los ciberataques [Acosta *et al*., 2009].

El grado de conocimiento que necesita un atacante para realizar una agresión a los sistemas de información ha decrecido a lo largo del tiempo, debido al aumento de la calidad, cantidad y disponibilidad de herramientas ofensivas. Actualmente, es relativamente fácil encontrar en internet herramientas de ethical hacking basadas en el uso de conocimientos de informática y seguridad para realizar pruebas en redes y encontrar vulnerabilidades, para luego reportarlas, sin hacer daño. Existen también herramientas de informática forense y de seguridad informática, entre otras, que son utilizadas con mala intención. Todo ello conforma un escenario de nuevos riesgos para el que es necesario que los distintos gobiernos desarrollen planes o estrategias, y se contemple la Ciberdefensa como un riesgo al que es preciso hacer frente para mejorar la seguridad nacional.

La forma de defenderse de estos ataques es compleja, dado que influyen diversos factores. Uno de ellos es el hecho de que muchos de los objetivos propensos a ser atacados se encuentran en manos de empresas privadas, por lo que su seguridad depende en gran medida de las acciones que toman éstas para asegurar sus sistemas, lo que implica asumir costos que en ocasiones no se están dispuestos a asumir, generando riesgos significativos. Otro factor importante es la falta de conciencia en seguridad de algunas partes de la sociedad, lo que dificulta tomar medidas eficaces y poder coordinarlas.

La Ciberdefensa se considera por lo tanto un ámbito de la Seguridad Nacional en el que los gobiernos deberán definir una estrategia, que deberá ejecutarse en coordinación con los sectores público y privado, ser compatible con los derechos y libertades individuales y ser coordinada con otras acciones para detectar las distintas amenazas, establecer sistemas de respuesta y recuperación ante eventualidades. Además se debe fomentar la cooperación internacional como punto clave para lograr tratados internacionales y la colaboración.

2.2. LA CIBERSEGURIDAD

A principios de 2011, un grupo de trabajo bilateral ruso-estadounidense del EastWest Institute (EWI) y la Universidad de Moscú elaboro un marco de terminología internacional. Definieron la Ciberseguridad como "una propiedad del ciberespacio, que tiene la capacidad de resistir las amenazas intencionales y no intencionales, responder y recuperarse" [Rauscher y Yashenko, 2011].

La Ciberseguridad se refiere generalmente a la capacidad de controlar el acceso a las redes, sistemas de información y todo tipo de recursos de información. Es decir donde los controles de Ciberseguridad son eficaces y el ciberespacio es considerado confiable, flexible y seguro para las ICIs. Sin embargo, donde los controles de Ciberseguridad están ausentes, incompletos, o mal diseñados, el ciberespacio es considerado como tierra de nadie.

Prevenir, detectar, responder y recuperarse se señalan como los objetivos de la Ciberseguridad, pero tradicionalmente el objetivo principal fue prevenir que se concrete un ataque exitoso. Sin embargo, todos los profesionales de seguridad son conscientes de que simplemente no es posible evitar todos los ataques y que debe existir una planificación y preparación que incluya métodos para detectar ataques en progreso, preferentemente antes de que causen daño. Una expectativa más positiva en Ciberseguridad, sería tener la capacidad de responder, y además también recuperar o corregir. En

cualquier caso, serán las lecciones aprendidas respecto de las respuestas a incidentes y la recuperación, las que alimentarán la planificación de la prevención.

En general se podría decir que la Ciberseguridad se refiere a métodos de uso, procesos y tecnologías para prevenir, detectar y recuperarse de daños a la confidencialidad, integridad y disponibilidad de la información en el ciberespacio.

Todas las partes involucradas en la ciberseguridad, ya sea un usuario individual de internet, un pequeño negocio, una institución, organismos públicos o empresas privadas, deben decidir su propia política para mantener la seguridad en el ciberespacio y estas deben estar directamente correlacionadas entre si y responder a una Estrategia Nacional de Ciberseguridad de nivel superior con una misión y un propósito como nación.

El desarrollo de Políticas o Estrategias de Ciberseguridad no es una tarea fácil, y no se basa solo en la aplicación de la ley, la gestión y la tecnología, requiere una forma consensuada y armoniosa de actuar y resaltar la necesidad de innovación.

Las naciones abordan el concepto de Ciberseguridad con distintos enfoques pero se debe tener en cuenta que enfrentan un mismo conjunto de amenazas y que se deberían emplear actividades de coordinación, como definiciones internacionales, terminología armonizada e intercambio de información. Debido a la naturaleza global del ciberespacio, podría esperarse que la colaboración internacional sea una de las más altas prioridades en una Estrategia Nacional de Ciberseguridad.

2.3 ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

Durante las últimas décadas, las nuevas tecnologías, los servicios electrónicos y de redes de comunicación se han integrado cada vez más a nuestra vida diaria. Las empresas, la sociedad, el gobierno y la defensa nacional dependen del funcionamiento de las TICs y de las ICIs. El transporte, las comunicaciones, el comercio electrónico, los servicios financieros, los servicios de emergencia y los servicios públicos se basan en la disponibilidad, integridad y confidencialidad de la información que fluye a través de estas infraestructuras.

Como se mencionó anteriormente a medida que la sociedad se vuelve más dependiente de las TICs, la protección y la disponibilidad de los servicios críticos se vuelven un tema de interés nacional.

Los incidentes que causan la interrupción de las infraestructuras críticas y de los servicios podrían causar importantes impactos negativos en la sociedad y en la economía. Asegurar el ciberespacio se ha convertido en uno de los retos más importantes de la actualidad y es considerado como una cuestión nacional a nivel estratégico que afecta a todos los niveles de la sociedad.

Por lo tanto una Estrategia Nacional de Ciberseguridad se define como "un plan de acción nacional sobre la base de una visión nacional para lograr un conjunto de objetivos que contribuyan a la seguridad del ciberespacio" [Luiijf *et al*., 2013]. Se encuentra a un alto nivel en la pirámide organizacional de una nación, y establece una serie de objetivos nacionales y prioridades que deben alcanzarse en un plazo determinado. Como tal, proporciona un marco estratégico para la implementación de un Sistema de Ciberseguridad Nacional, que se entiende como un conjunto de órganos, organismos y procedimientos que permiten la dirección, control y gestión de la Ciberseguridad.

El desarrollo de una estrategia integral puede plantear muchos desafíos, ya que es necesario lograr la cooperación y el acuerdo entre las partes interesadas, lograr un curso de acción común, y esta tarea no será fácil. Debe tenerse en cuenta que el proceso de desarrollo de la estrategia es probablemente tan importante como el documento resultante final.

Entonces, se puede decir que una Estrategia Nacional de Ciberseguridad (ENCS) es un instrumento para mejorar la seguridad y la resistencia de las ICIs y la continuidad de los servicios nacionales de información. En general, una ENCS tendrá los siguientes objetivos:

- Alinear acciones para trabajar de manera armoniosa.
- Coordinar la cooperación de los sectores público y privado.
- Transmitir directivas, responsabilidades y establecer relaciones entre todas las partes involucradas.

Los involucrados en el contexto de una (ENCS) son el gobierno, las agencias u organismos gubernamentales, los militares, organismos reguladores, los operadores de las ICIs, las industrias, los negocios en general, las pequeñas y medianas empresas (PYMEs), las organizaciones de investigación y desarrollo, las universidades, los ciudadanos y la población en general. Por consiguiente una ENCS debe describir actividades que se relacionaran con otras estrategias nacionales de orden superior, tales como la estrategia de seguridad y defensa nacional, la estrategia

nacional de protección de ICIs, la agenda digital nacional, la estrategia nacional de desarrollo económico, así como las estrategias internacionales.

En este trabajo se seleccionaron un conjunto de naciones que han desarrollado y publicado sus ENCS, como Australia (AUS), el Inglaterra (ENG versiones 2009 y 2011), Estados Unidos (EE.UU.), Alemania (ALE), Francia (FRA), España (ESP), Estonia (EST), Japón (JPN) y Rusia (RUS) con el objeto de analizar y realizar una comparación entre las mismas.

Por otro lado se propone seleccionar otras naciones latinoamericanas tales como Colombia (COL), Brasil (BRA), Chile (CHILE) y Argentina (ARG) que están trabajando en el desarrollo de una ENCS y que enfocaran el presente trabajo dentro del contexto socioeconómico de nuestro país.

Se van a tener en cuenta los principales aspectos en los que se enfocan la mayoría de los países que tienen implementadas sus ENCS, y que deben tenerse en cuenta en la elaboración de las Estrategias o Políticas de Ciberseguridad, para afrontar los riesgos del ciberespacio:

a) Protección de:

- Infraestructura crítica de información ICI: Es el conjunto de computadoras, sistemas computacionales, redes de telecomunicaciones, datos e información, cuya destrucción o interferencia puede debilitar o impactar en la seguridad de una nación.
- Economía: se refiere a la presencia de la economía en el ciberespacio, es una forma de organizar el intercambio de bienes y servicios empresa-empresa, empresa-cliente, sin importar su ubicación geográfica, ni las diferencias de tiempo. Las actividades más desarrolladas son e-commerce/e-business.
- Seguridad Nacional: noción de relativa estabilidad, calma y seguridad, beneficiosa para el desarrollo de un país, así como la implementación de los recursos y estrategias para conseguirla (principalmente a través de la defensa nacional).
- Bienestar Social: conjunto de factores que participan en la calidad de vida de las personas y que hacen que su existencia posea todos aquellos elementos que dan lugar a la tranquilidad y satisfacción humana.

b) Enfoque de la estrategia/política hacia:

- Concientización: campaña que se realiza con el objeto de que la sociedad tome conciencia sobre los riesgos individuales (privacidad e intimidad) y colectivos (seguridad nacional, prosperidad económica, social y cultural) que se derivan de un uso inadecuado del ciberespacio.
- Conocimiento: mantener un estado avanzado de conocimiento de la tecnología y de la situación del ciberespacio, establecer la vigilancia tecnológica en materia de Ciberseguridad que garantice la obtención de conocimiento y la promoción de proyectos de cooperación para lograr una integración y el máximo aprovechamiento de las oportunidades, los recursos y los avances internacionales.
- Educación: incorporar materias relacionadas con la Ciberseguridad en los planes de educación, esta formación debe iniciarse a temprana edad (educación primaria) y ser ampliada a lo largo de la educación secundaria, universitaria y post-universitaria. El objeto de iniciar la educación a temprana edad pretende, por un lado, homogeneizar los conocimientos en el uso de las nuevas tecnologías así como su uso responsable, y por otro lado, identificar a los futuros 'cibertalentos'.
- Capacidades cibernéticas militares: Capacidad de las fuerzas armadas de un país para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional.

c) Participación del sector público en la estrategia/política:

- Liderazgo: el ámbito y la complejidad de los desafíos del ciberespacio requieren, además de un liderazgo nacional, la adecuada coordinación de las capacidades, recursos y competencias involucradas. Ambas exigencias deben ser asumidas por el gobierno quien dirigirá y supervisará la Estrategia/Política de Ciberseguridad Nacional.
- Marco Jurídico: contar con un marco legislativo fuerte en el área de ciberseguridad, que trate los diferentes tipos de delitos tanto a nivel nacional como internacional. Además de la existencia de un marco regulatorio para la implementación de la Estrategia Nacional de Ciberseguridad.

d) Participación del sector privado en la estrategia/política:

- Participación en la estrategia/política: los actores en sectores claves como energía, transportes, entidades financieras, bolsas de valores, proveedores de servicios de internet, entre otros deben evaluar los riesgos que les afectan y mediante una adecuada gestión de los mismos asegurar que los sistemas de información y las redes son fiables y resistentes. Además deben asumir el

compromiso de compartir la información con las autoridades gubernamentales competentes en materia de Ciberseguridad.

e) Cooperación internacional:

- Cooperación en su grupo: se denomina grupo en este caso a un bloque geopolítico, que es la distribución conformada por países que comparten cierta extensión de tierra, panorama económico, político y cultural imperante. También se basa en la influencia que tiene un país sobre los demás, respecto del poder político, económico, militar, y que puede llegar a influenciar en la toma de decisiones de un país.
- Cooperación con otros países: la globalización tecnológica, sus oportunidades y sus riesgos obligan a alinear las iniciativas de todos los países que persiguen un ciberespacio seguro y confiable. Estos esfuerzos internacionales han de contemplar la elaboración y adopción de estándares globales, la expansión de la capacidad del sistema jurídico internacional y el desarrollo y la promoción de las mejores prácticas para generar sistemas de alerta y de respuesta a los ciberataques.

2.3.1. ESTRATEGIAS NACIONALES DE CIBERSEGURIDAD SELECCIONADAS

	BLOQUE GEOPOLÍTICO	ANGLOSAJÓN			UNIÓN EUROPEA					
	PAÍS	CAN	ENG	USA	ALE	FRA	ESP	EST	JPN	RUS
PROTECCIÓN	Infraestructuras criticas	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
	Economía		**X**	**X**	**X**		**X**		**X**	
	Seguridad Nacional	**X**	**X**	**X**	**X**	**X**	**X**		**X**	
	Bienestar social	**X**	**X**	**X**	**X**			**X**	**X**	**X**
ENFOQUE	Concientización	**X**	**X**	**X**				**X**		
	Conocimiento		**X**	**X**						**X**
	Educación		**X**	**X**				**X**		
	Capacidades cibernéticas militares		**X**	**X**	**X**	**X**				**X**
SECTOR PUBLICO	Liderazgo	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	
	Marco jurídico		**X**	**X**	**X**	**X**			**X**	**X**

SECTOR PRIVADO	Participación en la estrategia	X	X	X		X	X	X	X	X
COOPERACIÓN INTERNACIONAL	Cooperación en su grupo	X		X	X	X	X			
	Cooperación con otros países	X	X	X	X	X	X	X	X	X

Al analizar el cuadro comparativo, se puede observar como primera impresión que, los Estados Unidos, Inglaterra y Alemania tienen las ENCS más completas y son los actuales líderes mundiales en Ciberseguridad. En segundo lugar, los EE.UU. e Inglaterra disponen de un importante papel del sector privado como parte de sus estrategias, mientras que Alemania tiende a poner más énfasis en el sector público y en un fuerte marco legislativo regulatorio. En tercer lugar, y como es de esperar, los países se alinean en el ciberespacio de acuerdo a sus bloques geopolíticos.

Al analizar las ENCS de las naciones surge que la mayoría apunta a la prosperidad económica en el campo del ciberespacio, y que la ciberseguridad es considerada como un requisito para mejorar la prosperidad de la población y para fomentar el bienestar económico.

Se realizará un análisis de las ENCS desde diferentes puntos de vista:

1. Documentos publicados: es decir las ENCS publicadas en los respectivos sitios gubernamentales de cada país, en este apartado del trabajo solo se citará un extracto de los mismos.

   a) EEUU en su ENCS tiene cinco iniciativas estratégicas [United States Department of Defense, 2011]:

      Iniciativa Estratégica 1: Tratar el ciberespacio como un dominio operacional para organizar, entrenar y equipar a fin de que el Departamento de Defensa pueda aprovechar al máximo el potencial del ciberespacio.

      Iniciativa Estratégica 2: Emplear nuevos conceptos operativos de defensa para proteger redes y sistemas del Departamento de Defensa.

Iniciativa Estratégica 3: Asociarse con otros departamentos, agencias del gobierno y el sector privado para permitir una estrategia de Ciberseguridad global del gobierno.

Iniciativa Estratégica 4: Construir relaciones sólidas con los aliados de EE.UU. y los asociados internacionales para reforzar la Ciberseguridad colectiva.

Iniciativa Estratégica 5: Aprovechar el ingenio de la nación a través de una mano de obra excepcional y la rápida innovación tecnológica.

Asimismo a lo largo del documento se describen un conjunto de actividades basadas en un modelo de colaboración entre el gobierno, los socios internacionales y el sector privado:

- Economía: promover las normas internacionales y la innovación (los mercados abiertos).
- La protección de la infraestructura crítica: fortalecimiento de la seguridad, la confiabilidad y flexibilidad.
- Marco legal: extender la colaboración y el Estado de Derecho.
- Capacidades cibernéticas militares: preparación para los retos de seguridad.
- Desarrollo Internacional: creación de capacidad, seguridad y prosperidad.
- Bienestar social: apoyo de las libertades fundamentales y de privacidad.

b) La ENCS de Canadá se basa en tres pilares [Canada - Minister of Public Safety, 2010]:

Asegurar los sistemas de gobierno: tiene como objetivo establecer las funciones y responsabilidades claras, para reforzar la seguridad de los sistemas cibernéticos federales y para aumentar la conciencia de Ciberseguridad en todo el gobierno.

Alianzas para asegurar los sistemas cibernéticos vitales fuera del Gobierno federal: abarca una serie de iniciativas para asociarse con las provincias, territorios y la participación del sector privado con infraestructuras críticas.

Ayudar a los canadienses a estar seguros online: abarca la lucha contra la ciberdelincuencia y la protección de los ciudadanos canadienses en entornos online. Cuestiones de privacidad están especialmente dirigidas en este pilar.

c) La ENCS de Inglaterra se concentra en los objetivos nacionales vinculados a la evolución de la ciberseguridad, hacer de Inglaterra una potencia económica, fomentar la inversión y la calidad en el ámbito de las TICs y de esta manera aprovechar al máximo el potencial y las ventajas del ciberespacio. El objetivo es hacer frente a los riesgos derivados del ciberespacio, tales como los ciberataques de delincuentes, terroristas y de los estados, con el fin de que sea un espacio seguro para los ciudadanos y para las empresas.

Para alcanzar esta visión para el 2015, se basa en los siguientes objetivos [United Kingdom Minister for the Cabinet Office, 2011]:

Objetivo 1: hacer frente a la delincuencia cibernética y ser uno de los lugares más seguros del mundo para hacer negocios en el ciberespacio.

Objetivo 2: ser cada vez más resistente a los ataques cibernéticos y más capaces de proteger sus intereses en el ciberespacio.

Objetivo 3: ayudar a dar forma a un ciberespacio abierto, estable y vibrante que el público de Inglaterra pueda utilizar con seguridad y apoyar las sociedades abiertas.

Objetivo 4: tener todos los conocimientos, habilidades y capacidades que se necesitan para cumplir con todos los objetivos de Ciberseguridad.

Cabe destacar que Inglaterra es el más explícito en sus fuerzas armadas y en inteligencia, propicia la creación de capacidades en el dominio del ciberespacio.

d) La ENCS de Alemania se basa en las siguientes áreas estratégicas [Federal Ministry of the Interior, 2011]:

Protección de la infraestructura critica de información: El sector público y el privado deben crear una base estratégica y organizativa mejorada para una coordinación basada en el intercambio de información. Con la participación del Consejo Nacional de Ciberseguridad, se evalúa la integración de sectores adicionales y se considera la introducción de nuevas tecnologías donde las medidas protección deben ser obligatorias y dónde poderes adicional se requieren.

Sistemas informáticos seguros en Alemania: la protección de la infraestructura requiere más seguridad en lo que respecta a los sistemas informáticos utilizados por los ciudadanos y las Pymes. Los usuarios necesitan información apropiada y consistente sobre los riesgos relacionados con el uso de los sistemas informáticos y de las medidas de seguridad que pueden tomar para usar el ciberespacio de una manera segura.

Fortalecimiento de la seguridad de TI en la administración pública: las autoridades estatales tienen que servir como modelos para la seguridad de datos. Se creará una infraestructura común de red segura en la administración federal (Redes federales) como base para las comunicaciones.

Centro Nacional de Respuesta Cibernética: para optimizar la cooperación entre todas las autoridades estatales y mejorar la coordinación de las medidas de protección y respuesta a incidentes de TI se creó un Centro Nacional de Respuesta Cibernética que coordina la cooperación entre los organismos federales. El intercambio de información sobre las debilidades de los productos de TI, vulnerabilidades, formas de ataques y los perfiles de los autores permite que el Centro Nacional de Respuesta Cibernética pueda analizar los incidentes de TI y dar recomendaciones para la acción.

Consejo Nacional de Ciberseguridad: la identificación y eliminación de las causas estructurales de las crisis se consideran una importante herramienta de prevención para la Ciberseguridad. Para mantener la cooperación dentro del Gobierno Federal, entre el sector público y el sector privado se estableció un Consejo Nacional de Ciberseguridad.

Control eficaz del delito en el ciberespacio: las capacidades de las agencias de aplicación de la ley, la Oficina Federal de Seguridad de Información y el sector privado en la lucha contra el delito cibernético, deben reforzar su protección contra el espionaje y sabotaje. Para hacer frente a los crecientes desafíos de las actividades globales de delincuencia cibernética se debe lograr la armonización mundial en el derecho penal, basado en la Convención contra la Ciberdelincuencia del Consejo de Europa y examinar convenciones en esta área en el ámbito de la ONU (Organización de la Naciones Unidas).

Acción coordinada para garantizar la Ciberseguridad en Europa y en todo el mundo: la ciberseguridad mundial sólo puede lograrse a través de herramientas coordinadas a nivel nacional e internacional. A nivel de la Unión Europea (UE) se apoyan medidas adecuadas en

función del plan de acción para la protección de ICIs, la extensión y la ampliación del mandato de la Agencia de Seguridad de la Información de la Red Europea (ENISA). En el marco del G-8 (grupo informal de países del mundo cuyo peso político, económico y militar es relevante a escala global y que está conformado por Rusia, Canadá, Estados Unidos, Francia, Italia, Alemania, Reino Unido y Japón, se trabaja actualmente en intensificar las actividades de lucha contra las botnets, que se conocen como redes de robots informáticos o bots, que se ejecutan de manera autónoma, automática, controlados remotamente y que usan para diversas actividades criminales.

Uso de TICs fiable y de confianza: la disponibilidad de los sistemas informáticos fiables debe garantizarse de forma permanente. Se pretende fortalecer la soberanía tecnológica y la capacidad económica en todas las competencias estratégicas de TI y se favorece la diversidad tecnológica. El objetivo es utilizar componentes en áreas críticas de seguridad que son certificadas frente a un estándar de certificación reconocido internacionalmente.

Desarrollo personal en las autoridades federales: se intensificó el intercambio de personal entre las autoridades federales y el empleo de las medidas apropiadas de formación para fortalecer la cooperación interministerial.

Herramientas para responder a los ataques cibernéticos: un coordinado e integral conjunto de herramientas para responder a los ataques cibernéticos se debe crear en cooperación con las autoridades estatales competentes.

Cabe destacar que Alemania se centra en la prevención y el enjuiciamiento de los ataques cibernéticos y se enfoca en el desarrollo de operaciones cibermilitares.

e) La ENCS de Francia se basa en los siguientes objetivos [Secretary General for Defence and National Security, 2011]:

Convertirse en una potencia mundial en Ciberdefensa: mientras mantiene su independencia estratégica, Francia debe trabajar para asegurarse de que pertenece al círculo íntimo de los países líderes en el área de la Ciberdefensa. Por lo tanto se debe buscar el beneficio de la cooperación a nivel operativo y en la aplicación de una estrategia unificada para hacer frente a las amenazas.

Salvaguardar la capacidad de Francia para tomar decisiones a través de la protección de la información relacionada con su soberanía: las autoridades gubernamentales y actores de gestión de crisis deben tener los recursos para comunicarse en cualquier situación y en total confidencialidad. Se debe garantizar la confidencialidad de la información que circula en estas redes, para ello se requieren productos de seguridad adecuados y se debe tener la experiencia necesaria para diseñarlos y optimizar sus métodos de desarrollo y producción.

Fortalecer la Ciberseguridad de las infraestructuras críticas nacionales: en colaboración con los fabricantes y operadores de equipos, el Estado debe trabajar para garantizar y mejorar la seguridad de estos sistemas críticos.

Garantizar la seguridad en el ciberespacio: las amenazas a los sistemas de información afectan simultáneamente a los servicios públicos, privados, a empresas y ciudadanos. Los servicios públicos deben operar de manera ejemplar y mejorar la protección de sus sistemas de información, las campañas para recaudar información y la concientización se debe dirigir a las empresas y a los ciudadanos. En cuanto a la lucha contra el delito cibernético, Francia promoverá el fortalecimiento de la legislación vigente y la cooperación judicial internacional.

Para cumplir estos objetivos, se han identificado siete áreas de actuación:

- Anticipar y analizar efectivamente el entorno con el fin de hacer apropiada la toma de decisiones.
- Detectar y bloquear ataques, alertar y apoyar a las potenciales víctimas.
- Mejorar las capacidades científicas, técnicas e industriales.
- Proteger los sistemas de información del Estado y los operadores de las ICIs para garantizar una mejor capacidad de recuperación nacional.
- Adaptar la legislación francesa para incorporar avances tecnológicos y nuevas prácticas.
- Desarrollar iniciativas de colaboración internacional en las áreas de seguridad de sistemas de información, la Ciberdefensa y lucha contra la delincuencia informática con el fin de proteger los sistemas de información nacionales.
- Comunicar, informar y convencer a la población de la magnitud de los desafíos relacionados con los sistemas de seguridad de la información.

Francia se destaca por los medios técnicos empleados para mantener la seguridad de los sistemas de información y la lucha contra la ciberdelincuencia. Se enfoca en su seguridad nacional y en la estrategia de defensa que establece la necesidad de defensa militar cibernética y la disuasión.

f) La ENCS de España se sustenta en los siguientes principios [Departamento de Seguridad Nacional – Presidencia del Gobierno, 2013]:

Liderazgo nacional y coordinación de esfuerzos: el ámbito y la complejidad de los desafíos del ciberespacio requieren, además de un liderazgo nacional decidido, la adecuada coordinación de las capacidades, recursos y competencias involucradas. Ambas exigencias son asumidas por el Presidente del Gobierno quien dirigirá y supervisará la Política de Ciberseguridad Nacional en el marco del Consejo de Seguridad Nacional.

Responsabilidad compartida: todos los agentes públicos y privados con responsabilidad en esta materia, incluyendo también a los propios ciudadanos, han de sentirse implicados con la Ciberseguridad. Para ello, se hace precisa una intensa coordinación de los diferentes organismos de las Administraciones Públicas y una adecuada cooperación público-privada capaz de compatibilizar iniciativas y propiciar el intercambio de información.

Proporcionalidad, racionalidad y eficacia: es necesario gestionar los riesgos derivados del uso de la tecnología de forma dinámica, equilibrando oportunidades y amenazas, asegurando la proporcionalidad en las medidas de protección adoptadas, que habrán de ser elementos habilitantes de la confianza y no trabas al desarrollo de nuevos servicios.

Cooperación Internacional: el carácter transfronterizo de las amenazas hace que sea esencial promover la cooperación global, ya que muchas de las posibles medidas sólo resultarán eficaces si se adoptan internacionalmente con la adecuada cooperación y coordinación entre los distintos países.

g) La ENCS de Estonia [Ministry of Economic Affairs and Communication, 2014], se basa en un objetivo general de cuatro años que consiste en aumentar las capacidades de ciberseguridad y sensibilizar a la población de las amenazas informáticas, garantizando la confianza en el ciberespacio.

Además se plantean los siguientes sub-objetivos:

Garantizar la protección de los sistemas de información de servicios importantes: El funcionamiento del Estado de Estonia y la sociedad, la economía y el bienestar social de todas las personas, la vida y la salud dependen cada vez más de la seguridad de los sistemas y servicios. Uno de los principales objetivos de la estrategia es describir los métodos para asegurar la ininterrumpida operación y la capacidad de recuperación de los servicios vitales, y la protección de las ICIs contra las amenazas cibernéticas.

Mejorar la lucha contra la ciberdelincuencia: El daño económico derivado de la ciberdelincuencia reduce la confianza en los servicios digitales y en el peor de los casos podría llevar a la pérdida de la vida. Una mayor conciencia del público en general acerca de los riesgos de la Ciberseguridad ayuda a prevenir los delitos cibernéticos. Una mayor conciencia se logra abordando temas relacionados en todos los niveles de la educación e informando a las personas sobre la base de la investigación y el análisis de los comportamientos seguros.

Desarrollo de las capacidades de ciberdefensa nacional: organizaciones civiles, militares, y la cooperación internacional ponen los recursos a disposición del Estado. Esto debe funcionar adecuadamente en el ciberespacio, con respecto a la advertencia, la disuasión y la defensa activa.

Estonia debe gestionar la evolución de las amenazas de ciberseguridad: para mantener y mejorar su capacidad de Ciberseguridad, adoptará soluciones de Ciberseguridad independientes, que son respaldadas por las oportunidades de capacitación y formación en Ciberseguridad, investigación, desarrollo y el espíritu empresarial. Con el fin de garantizar el sostén de las soluciones de seguridad, el Estado actúa como contratista inteligente, y apoya la exportación de las soluciones de ciberseguridad.

h) La ENCS de Japón se basa en cuatro principios básicos [Information Security Policy Council, 2013]:

Garantizar la libre circulación de la información: se trabaja para construir un ciberespacio seguro y confiable en que el libre flujo de información está garantizado asegurando la apertura e interoperabilidad del ciberespacio, sin excesivamente administrarlo o regularlo. Como resultado, el ciberespacio proporcionará una variedad de beneficios incluida la

innovación, el crecimiento económico y las soluciones para los problemas sociales, mientras se garantiza la libertad de expresión y la protección de la privacidad.

Responder a los riesgos cada vez más graves: los riesgos para el ciberespacio continúan avanzando y la respuesta inmediata es necesaria. Por esta razón, se deben adoptar medidas de seguridad individuales, medidas para eventualidades y la preparación de sistemas de respuestas, es decir es necesario un nuevo mecanismo a través de esfuerzos en varias capas, como un sistema social que pueda abordar con urgencia y de manera adecuada el cambio riesgos asociados con la evolución en las TICs y otros factores.

Mejorar el enfoque basado en el riesgo: es necesario continuar con las medidas que se llevan a cabo por cada actor individual, a la vez aplicar de forma dinámica una asignación adecuada y oportuna de los recursos, como ser un mecanismo social para responder a los riesgos cambiantes. Se deben mejorar las funciones de reconocimiento y análisis de incidentes relacionados a los ciberataques y avanzar en el análisis de las capacidades de las amenazas, promoviendo el intercambio de información, el fortalecimiento de la cooperación entre CSIRT (Equipo de Respuesta ante Emergencias Informáticas de sus siglas en ingles Computer Security Incident Response Team) nacionales y CSIRT internacionales.

Asociación basada en responsabilidades compartidas: diversas entidades tales como el gobierno, el sector público, academias, industrias y sectores privados deben adoptar sus propias medidas de seguridad de la información en forma independiente y proactiva como parte de sus responsabilidades de desarrollo social, para garantizar un ciberespacio resistente y vigoroso líder en el mundo. Especialmente, como los riesgos se vuelven más generalizados, es importante que el conjunto de la sociedad participe en la limpieza del ciberespacio como medida de seguridad de la información preventiva contra intrusiones no autorizadas, las infecciones de malware y vulnerabilidades. En este sentido, las diversas partes interesadas en el ciberespacio tienen que cumplir con sus responsabilidades, que corresponden con sus respectivos roles en la sociedad, mientras que cooperan mutuamente y ayudan a la colaboración entre los sectores público y privado y la colaboración internacional.

f) La Doctrina de Seguridad de la Información de la Federación RUSA se basa en los siguientes principios [President of the Russian Federation, 2000]:

El cumplimiento de los derechos constitucionales y las libertades del ciudadano para utilizar la información: implica la preservación y el fortalecimiento de los valores morales de la sociedad y las tradiciones como el patriotismo, además de aumentar el potencial cultural y científico del país.

Soporte de información para la política estatal de la Federación Rusa: implica transmitir información confiable al público ruso e internacional, acerca de la política estatal de la Federación de Rusa y su posición oficial sobre los acontecimientos de importancia social. Esto se logra con permitir el acceso de los ciudadanos a los recursos de información del gobierno.

La promoción de las tecnologías modernas de información: impulsar la industria de la información (informática, telecomunicaciones e instalaciones de comunicaciones en particular), asegurar la satisfacción de las necesidades del mercado nacional con productos propios, como así también la entrada en el mercado mundial. Rusia debe ocupar una digna posición en el mundo, dentro de la industria micro-electrónica e informática.

2. Bloques geopolíticos:

a) El bloque anglosajón, liderado por los EE.UU. e Inglaterra, hace hincapié en un papel importante del sector privado, una fuerza laboral educada, la concientización y la diplomacia.

b) La Unión Europea, liderada por Alemania, se centra en un robusto marco jurídico y reglamentario, y en la promoción como modelo para la cooperación internacional de la "Convención sobre la Ciberdelincuencia de Budapest", que es el primer tratado internacional que busca hacer frente a los delitos informáticos y los delitos en internet mediante la armonización de leyes nacionales, la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones. Fue elaborado por el Consejo de Europa en Estrasburgo y firmado el 8 de noviembre de 2001, con la participación activa de los estados observadores de Canadá, Japón y China.

3. El marco legal

El carácter internacional del ciberespacio es un desafío a la Ciberseguridad, visto como una conexión de redes de computadoras que se encuentran físicamente en diferentes países, con distintas jurisdicciones legales, y ningún país puede dictar o controlar las interacciones en el ciberespacio. Por lo tanto, los países tratan de entrar en acuerdos internacionales, ya sean bilaterales o multilaterales en un esfuerzo para regular el ciberespacio y coordinar la Ciberseguridad, pero estos intentos son a menudo guiados por otros intereses que no siempre se corresponden con las respuestas más eficaces a la ciberdelincuencia.

Los intentos de coordinar la aplicación de la ley en distintas jurisdicciones son difíciles. En primer lugar, las jurisdicciones son soberanas, por lo tanto una jurisdicción tiene que reconocer que las pretensiones de otra jurisdicción son legítimas y dignas de apoyo.

En segundo lugar, las normas de procedimiento tienen que ser acordadas, estos acuerdos son más fáciles de alcanzar entre los países que comparten sistemas legales similares, tales como el sistema de Derecho Anglosajón, pero más difícil que se alcance entre países que no comparten estas similitudes.

En tercer lugar, suponiendo que un resultado legal favorable se ha logrado, la cooperación debe estar asegurada y es difícil de coordinar la ejecución práctica de una decisión judicial, como por ejemplo:

- La detención de un criminal
- El cobro de multas a organismos gubernamentales

4. Convenios o tratados multilaterales

El Convenio del Consejo de Europa de Budapest sobre la Ciberdelincuencia es el acuerdo líder multilateral sobre los delitos informáticos, con 32 países que han ascendido en el tratado y otros 15 los países que han firmado pero aún no ratificado. Cabe destacar que Rusia es el miembro más prominente del Consejo que no ha firmado el tratado y Japón no ha ratificado el tratado todavía. Si bien la Convención se está promoviendo por muchos países europeos, para los Estados Unidos se ve como la mejor opción para asegurar un acuerdo internacional sobre la lucha contra la ciberdelincuencia.

Aunque existe un amplio apoyo internacional a varias secciones de la Convención, como los relacionados con el fraude, la explotación infantil, la integridad de los ordenadores y las redes, dos áreas en particular siguen siendo polémicas [Luiijf *et al*., 2013]:

- Artículo 10, que se centra en los delitos relacionados con infracción del derecho de autor y los derechos de propiedad intelectual, fue rechazado por los países en desarrollo y por otros países que lo ven servir a intereses corporativos.

- Rusia ha expresado su inquietud por el artículo 32 (b), que permite a las agencias de un país de aplicación de la ley acceder a los datos en otro país, autorizado por empresas o particulares, sin el consentimiento expreso de las autoridades gubernamentales.

Más allá de los desafíos para la adopción universal de la Convención de Budapest, hay algunas limitaciones en el propio acuerdo:

En primer lugar, los cambios significativos en la tecnología y el malware se producen de forma continua desde que la Convención se publicó en el año 2001, esto implica una adaptación continua al cambio.

En segundo lugar, los recursos limitados, tanto en la financiación y el capital humano siguen siendo un problema en los países desarrollados y en los países en desarrollo. La ayuda de países, especialmente de los EE.UU. sigue mejorando la lucha contra la ciberdelincuencia, pero se necesitarán mayores capacidades de aplicación de la ley y mayores esfuerzos coordinados.

Para concluir el análisis de las ENCS en esta primera etapa, entre las problemáticas que no se pueden observar en el cuadro comparativo, se puede mencionar que la localización de orígenes y destinos de las amenazas informáticas es complicado. Se puede observar que potencias en Ciberseguridad, tales como Estados Unidos, Inglaterra y Alemania no sólo pueden ser el blanco de ataques, sino también la fuente de la actividad criminal, lo que deja una gran incertidumbre respecto de los orígenes de los ataques.

2.3.2. POLÍTICAS NACIONALES DE CIBERSEGURIDAD SELECCIONADAS

Muchos países miembros de la OEA (Organización de Estados Americanos) iniciaron sus esfuerzos en materia de Ciberseguridad con el establecimiento de Equipos de Respuestas ante Emergencias Informáticas de sus acrónimos en inglés Computer Emergency Response Team (CERTs). Se eligieron los principales estados Latinoamericanos competentes en el tema de la Ciberseguridad y la Argentina en particular para analizar su situación actual en Ciberseguridad.

La mayoría de los países de Latinoamérica, exceptuando a algunos del Caribe, disponen de capacidad de respuesta a incidentes a nivel nacional. Estos CERTs presentan todo un espectro en cuanto a su desarrollo, algunos prestan distintos servicios de respuesta y prevención de incidentes, mientras que otros todavía están enfrentando dificultades para proteger sus redes. Los problemas que enfrenta este último grupo se complican por las dificultades para obtener recursos humanos y financieros, lo que impide que mejoren sus operaciones.

La respuesta a incidentes representa solamente un área de la Ciberseguridad en que los Estados de América Latina han exhibido progresos significativos. Muchos están siguiendo la tendencia reciente establecida por países como Canadá, Estonia, Alemania, Japón, Inglaterra y Estados Unidos y han empezado a redactar políticas y estrategias nacionales integrales de Ciberseguridad. Con el apoyo de la OEA, Colombia se convirtió en el primer país latinoamericano en adoptar una Estrategia Nacional Integral de Ciberseguridad y Ciberdefensa. En términos globales, los Estados miembros de la OEA han mostrado unidad cuando se trata de asuntos de Ciberseguridad.

Mientras que la UE adoptaba una Estrategia de Ciberseguridad en febrero de 2013, los Estados miembros de la OEA ya habían adoptado por unanimidad la Estrategia Interamericana Integral de Ciberseguridad nueve años antes, en 2004. Conforme fue evolucionando el panorama de las amenazas, los esfuerzos de los gobiernos también lo hicieron, aprobaron una declaración sobre el "Fortalecimiento de la Ciberseguridad en las Américas" en marzo de 2012. La adopción de estos documentos prueba que aunque todavía queda mucho por hacer y los Estados intercambian distintas opiniones sobre la mejor forma de lograr la Ciberseguridad, existe un consenso político sólido en el Hemisferio Occidental, lo que ayuda a facilitar la cooperación regional y el intercambio de información. Trabajando con la OEA y a través de ella, los Estados miembros han logrado llegar a un consenso sobre el tema. Los acuerdos han generado un entorno colaborativo y en última

instancia han permitido que la Secretaría General de la OEA, suministre asistencia técnica y mejore la Ciberseguridad de los Estados miembros en múltiples niveles.

Por otro lado, las respuestas de los Estados miembros de la OEA a la ciberdelincuencia siguen siendo desiguales. Muchos gobiernos empezaron a tomar medidas serias para fortalecer la Ciberseguridad, tras la adopción de la Estrategia de Ciberseguridad de la OEA en 2004. En términos globales, los dirigentes políticos son conscientes de los peligros que plantean los hackers y los delincuentes cibernéticos para el desarrollo y la seguridad pública. Sin embargo, la voluntad política no siempre conduce a cambios en la situación imperante. En Latinoamérica, dos factores bloquean comúnmente los esfuerzos de los estados miembros:

- La falta de recursos dedicados al fortalecimiento de la capacidad en Ciberseguridad.
- La escasez de conocimientos especializados y experiencia práctica para la implementación de políticas y capacidades técnicas.

Latinoamérica sigue enfrentando restricciones presupuestarias, y los planes de gastos a menudo no contemplan grandes inversiones en aspectos como la seguridad informática. Los fondos se invierten con mayor frecuencia en aspectos de seguridad propiamente dicha, aunque esto probablemente cambiará conforme los riesgos cibernéticos vayan planteando cada vez más amenazas contra el bienestar físico, económico y la estabilidad de los gobiernos. En cualquier caso, es importante observar que a pesar de las limitantes presupuestarias, los países pueden dar grandes pasos en materia de Ciberseguridad.

Es importante mencionar la gran cantidad de software gratuito de Ciberseguridad a que tienen acceso los países, aunque no siempre logran aprovechar estas oportunidades. La escasez de conocimientos especializados y experiencia práctica necesaria para implementar iniciativas, podría atribuirse a las bajas tasas de matrícula en programas de formación técnica. En consecuencia, la falta de expertos calificados, implica que los países prácticamente no tengan capacidad para aprovechar el software libre con fines de Ciberseguridad. Algunos países experimentan esta deficiencia más que otros, pero este problema podría mitigarse mediante cooperación internacional. La OEA sigue promoviendo las relaciones y facilitando el intercambio de prácticas óptimas y conocimientos profesionales entre sus Estados miembros.

Dentro del contexto de estas deficiencias, los países latinoamericanos están luchando para sensibilizar a sus ciudadanos y están enfrentando dificultades para impulsar la implementación de

soluciones técnicas y políticas para los problemas de Ciberseguridad. Algunos gobiernos no tienen un manejo centralizado de información sobre los incidentes cibernéticos y no tienen capacidad para responder a incidentes. Incluso los que ya han dado algunos pasos, experimentan problemas con el intercambio de información entre sus ministerios y departamentos gubernamentales.

A continuación se mostrara un cuadro comparativo de las Políticas de Ciberseguridad empleadas por los Estados latinoamericanos seleccionados:

	BLOQUE GEOPOLÍTICO	OEA			
	PAÍS	COL	BRA	CHILE	ARG
PROTEGE	Infraestructuras criticas	**X**	**X**	**X**	**X**
	Economía		**X**		
	Seguridad Nacional		**X**		
	Bienestar Social	**X**	**X**		
ENFOQUE	Concientización	**X**	**X**	**X**	
	Conocimiento		**X**		
	Educación	**X**	**X**	**X**	
	Capacidades cibernéticas militares	**X**			
SECTOR PUBLICO	Liderazgo/coordinación	**X**	**X**	**X**	**X**
	Marco jurídico	**X**			**X**
SECTOR PRIVADO	Participación en la estrategia	**X**	**X**	**X**	
COOPERACIÓN INTERNACIONAL	Cooperación en su grupo	**X**	**X**	**X**	**X**
	Cooperación con otros países	**X**	**X**	**X**	**X**

Como análisis del cuadro comparativo se puede observar que Colombia junto con Brasil son las naciones más completas en el área de Ciberseguridad. Cabe destacar que Colombia es el único país en Latinoamérica que ha implementado un marco jurídico sostenible (Estrategia Integral de Ciberseguridad y Ciberdefensa). Por otro lado Brasil, si bien no tiene implementada una Estrategia de Ciberdefensa Nacional, tiene una política robusta que le permite posicionarse como un país con capacidades de Ciberdefensa y Ciberseguridad. Por último Chile, aunque no tiene ninguna

estrategia o política oficial en materia de Ciberseguridad a nivel nacional, en los últimos años las autoridades chilenas han trabajado en el desarrollo de una capacidad nacional de respuesta y gestión de incidentes cibernéticos. En este emprendimiento, han adoptado un enfoque bastante singular, ya que en lugar de concentrarse en la creación de un único CERT o un organismo similar, han concentrado sus esfuerzos en el desarrollo de procedimientos y mejores prácticas estandarizados en materia de gestión de incidentes y Ciberseguridad en general.

Puntualmente en cada país, se puede observar que:

a) COLOMBIA:

Adoptó en el año 2011 una Estrategia Integral de Ciberseguridad y Ciberdefensa conocida como el "CONPES 3701". Los aspectos técnicos de la Ciberseguridad y la Ciberdefensa del CONPES están a cargo de tres instituciones:

El Centro Cibernético Policial (CCP): responsable de asegurar la integridad de las redes policiales y de la sociedad civil, y que mantiene una vigorosa capacidad de investigación.

El Comando Conjunto Cibernético (CCOC): una unidad militar que responde a ataques contra los bienes militares de la nación.

El colCERT: la entidad coordinadora a nivel nacional que supervisa todos los aspectos de la Ciberseguridad y la Ciberdefensa.

En cuanto a la cooperación y el intercambio de información entre el sector privado y las autoridades gubernamentales, existe una norma específica, el Decreto 1704 (2012), que establece los requisitos que deben cumplir los proveedores de redes y servicios de telecomunicaciones a fin de respaldar, de manera eficaz y oportuna el trabajo de las autoridades nacionales. Además, las autoridades nacionales procuraron forjar relaciones con entidades claves del sector privado con el objeto de incrementar aún más la cooperación y el intercambio de información.

La cooperación internacional ha sido sólida, puesto que las autoridades nacionales colaboraron, de modo directo, con otras naciones en la respuesta a ataques cibernéticos o delitos cibernéticos. Un ejemplo de esto fue la participación activa de las autoridades colombianas en una iniciativa

multinacional, bajo el auspicio del Grupo de Trabajo Latinoamericano sobre Delitos Tecnológicos de INTERPOL, cuyo objeto era identificar y arrestar a los usuarios de foros online donde se intercambiaba y distribuía material sobre pedofilia. Entre los países que colaboraron, se encuentran Argentina, Brasil, Chile, Costa Rica, Ecuador, Uruguay, Venezuela y España.

b) BRASIL:

Ha desarrollado capacidades avanzadas en materia de Ciberseguridad y disuasión de delitos cibernéticos, y cuenta con una gran cantidad de instituciones y organismos en el área. La Policía Federal (DPF) es el principal organismo responsable de investigar todos los delitos perpetrados en el país y como tal, es la principal autoridad en materia de delitos cibernéticos, a través de su Servicio de Represión de Delitos Cibernéticos (SRCC). Asimismo, mantiene un segundo grupo de tareas especializado en la lucha contra los delitos relacionados con la pornografía infantil en internet (GECOP). Cuando la naturaleza de un delito informático en especial lo amerita, se da participación al personal de otras unidades del DPF y de otras instituciones.

Las autoridades nacionales, especialmente dentro del Departamento de Seguridad de la Información y Comunicaciones (DSIC), del Gabinete de Seguridad Institucional (GSI) de la Presidencia de la Nación, han desarrollado e implementado campañas de concientización para promover el uso inteligente y responsable de Internet por parte de los ciudadanos.

Si bien las entidades del sector privado no están legalmente obligadas a brindar a las autoridades nacionales información relativa a incidentes, las autoridades informaron que la cooperación entre ambos sectores es habitual y sólida. Como ejemplo, podemos mencionar un acuerdo entre el DPF y Microsoft, en virtud del cual Microsoft brinda al DPF la información de registro de los usuarios de sus servicios, cuando éste se lo solicita a través de un formulario electrónico. Las autoridades también señalaron que Brasil cuenta con un sector importante y productivo dedicado a desarrollar software de Ciberseguridad personalizado para entidades privadas, como bancos, y para instituciones públicas.

c) CHILE:

Varios organismos dentro del gobierno chileno comparten responsabilidades relativas a la promoción de la Ciberseguridad y la lucha contra los delitos cibernéticos. El Ministerio del Interior y Seguridad Pública, la Secretaría General de la Presidencia y la Subsecretaría de

Telecomunicaciones tienen un papel clave en materia de Ciberseguridad. Los Carabineros, o la policía nacional, son los encargados de las cuestiones relativas a los delitos cibernéticos, a través de su Departamento de Investigación de Organizaciones Criminales (OS-9). La Sección de Delitos de Alta Complejidad es parte de la estructura operativa del OS-9 y lidera las investigaciones relativas a las TICs o a la recolección y análisis de evidencia digital.

La capacidad Nacional de Respuesta y Gestión de incidentes cibernéticos, se encuentran delineados en el Decreto Supremo Número 1299 (Programa para la Mejora de la Gestión de Sistemas de Seguridad de la Información). Si bien el gobierno cuenta con un CERT desde 2004, llamado CERT-CL, no se trata de una entidad institucional formal sino de una función y estructura operativa mantenida por el Ministerio del Interior y Seguridad Pública. Sus metas incluyen ofrecer respaldo en materia de delitos cibernéticos a la Red de Conectividad del Estado y otras entidades del gobierno central, y promocionar la cooperación nacional e internacional, así como la concientización y el fortalecimiento de leyes y políticas nacionales.

La legislación chilena no obliga a las empresas privadas a compartir información relativa a incidentes con las autoridades nacionales, a menos que se requiera esta información como parte de una investigación penal oficial. Sin embargo, las autoridades nacionales procuran de forma activa desarrollar y mantener canales de comunicación con entidades claves del sector privado, cuya cooperación es esencial para llevar a cabo investigaciones o gestión de incidentes. Se informó que estos canales en general son a nivel operativo y que si bien pueden facilitar y acelerar el flujo de información, no cuentan con el beneficio de las estructuras o mecanismos institucionales que puedan facilitar estos intercambios.

El Ministerio de Educación ha desarrollado y está implementando, en asociación con varias entidades del sector privado, una campaña a largo plazo llamada “Internet Segura”, para concientizar y promover una cultura de Ciberseguridad.

d) ARGENTINA:

El gobierno argentino estableció la Oficina Nacional de Tecnologías de Información (ONTI) para evaluar y poner en marcha un sistema de modernización y uso eficiente de los recursos digitales. A través de esta Oficina se estableció en 2005 el Equipo de Respuesta ante Emergencias Informáticas (ArCERT), que hizo de Argentina uno de los primeros países en América Latina en operar un CERT nacional.

Para mitigar las amenazas emergentes a los sistemas de control industrial, en 2012 Argentina creó el (ICIC) Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad, al que se le ha encargado específicamente la protección de las ICIs del país, dependiente de la Jefatura de Gabinete de Ministros.

Actualmente, los cuatro objetivos principales de ICIC-ArCERT son los siguientes:

- Servir como repositorio de información relevante relacionada con los incidentes, herramientas y técnicas de ciberseguridad.
- Promover la coordinación entre los administradores de redes para todas las instituciones públicas a nivel nacional, a fin de prevenir, detectar, gestionar y recuperarse de los incidentes relacionados con la seguridad que afecten sus redes.
- Centralizar la generación de informes respecto a incidentes que afecten las redes gubernamentales y facilitar el intercambio de información a fin de abordarlos de manera más eficaz.
- Interactuar con otros equipos de respuesta ante incidentes en el país y la región.

La ONTI está trabajando actualmente en el segundo borrador del Plan Nacional de Ciberseguridad y Protección de Infraestructura Crítica 2013-2015. Este plan se basa en cuatro pilares:

- Sensibilización.
- Protección de los activos digitales.
- Promoción de la comprensión judicial y académica de la seguridad de la información y de las ICIs.
- Fomento de alianzas de seguridad duraderas entre el gobierno, las empresas y las organizaciones de la sociedad civil.

La investigación de los delitos cibernéticos y las actividades relacionadas es llevada a cabo principalmente por la Policía Federal Argentina (PFA), a través de su División de Delitos Tecnológicos.

Se debe mencionar que las empresas del sector privado no están obligadas por ley a proporcionar información relacionada con los incidentes a las autoridades nacionales. No

obstante, las autoridades han informado que existen mecanismos establecidos para facilitar el intercambio de información por parte de las empresas privadas, como los proveedores de Internet (ISP) o de servicios de correo electrónico, cuando existe una clara base legal y judicial para la investigación. La actual legislación relacionada con los delitos informáticos se aprobó en 2008 y ha permitido realizar investigaciones y procesamientos exitosos en varios casos de importancia. No obstante, las autoridades indicaron que sus esfuerzos para hacer pleno uso de la ley para combatir los delitos cibernéticos han sido obstaculizados en cierto modo, por los desafíos que surgen de la naturaleza de los delitos informáticos, que no tienen fronteras y están en constante evolución.

El ICIC ha desarrollado una iniciativa llamada "Internet Sano", que apunta a promover el uso responsable de las TICs e Internet y la Dirección Nacional para la Protección de Información Personal, dependiente del Ministerio de Justicia y Derechos Humanos, ha desarrollado un segundo programa de concientización denominado "Contigo en la web". En la actualidad, varias instituciones de educación superior en Argentina ofrecen programas de certificación y de grado en una amplia variedad de aspectos relacionados con la Ciberseguridad, incluyendo el análisis forense digital. Asimismo, se informó que el Instituto Nacional de Administración Pública (INAP) ofrece capacitación y cursos sobre temas relacionados con Ciberseguridad. Aunque no se cuenta con registros detallados y cifras concretas disponibles para su distribución pública, las autoridades nacionales han observado durante 2014 un aumento en determinados delitos informáticos y otras actividades informáticas maliciosas, entre los que se incluyen: suplantación de identidad y fraudes por medio de las redes sociales, el correo electrónico o la banca electrónica, mediante el uso de ingeniería social, keyloggers, malwares y herramientas persistentes avanzadas APT. Sin embargo, no existe información disponible que indique qué sector de la población ha sido el más afectado o perjudicado.

2.3.3.LA CIBERSEGURIDAD NACIONAL ARGENTINA

El Gobierno argentino tiene el propósito de prepararse ante las amenazas cibernéticas emergentes, desde el año 2012 ha llevado a cabo Ejercicios Nacionales de Respuesta a Incidentes Cibernéticos (ENRIC), los cuales se realizan de forma anual. Durante el año 2014, el ejercicio fue realizado conjuntamente por la ONTI/ICIC, el Ministerio de Defensa y la Armada Argentina. Otros talleres sobre tecnologías emergentes de Ciberseguridad se llevan a cabo de forma regular para garantizar que el personal técnico permanezca al día sobre las últimas tendencias.

Pero se identificaron tres dificultades principales a sus iniciativas relacionadas con la seguridad y los delitos cibernéticos, específicamente:

- La falta de concientización entre las partes involucradas en un Sistema de Seguridad Nacional.
- La falta de un marco legal estable.
- Presupuesto insuficiente para llevar adelante las iniciativas.

A lo mencionado anteriormente se suma el largo historial de ataques a sus sitios web que tiene la Argentina, aunque no en la medida de otros países como Rusia, Estonia, Georgia, China o Estados Unidos, los cuales ya se ven involucrados en algunas de las llamadas ciberguerras, debido a sus rivalidades políticas.

A continuación se hará un breve recorrido por los principales tipos de ataques producidos en nuestro país, con una breve descripción de los mismos. Los casos presentados fueron extraídos de [Borghello y Temperini, 2013].

a) Modificación de sitios y/o base de datos

Quizás uno de los casos más conocidos y resonantes de los últimos años fue el que se produjo en junio de 2009, cuando, en plenas elecciones legislativas, se ingresó a la base de datos del padrón electoral y se agregaron leyendas ofensivas sobre algunas provincias. El sitio fue corregido pero, luego de que las primeras leyendas fueran suprimidas, volvieron a ingresar al sitio, perteneciente al Poder Judicial de la Nación, para escribir: "aumenten la seguridad" (Figura1).

Figura 1: Ataque al sitio del padrón electoral de Argentina el 26/06/2009.

Un incidente de mayor relevancia sucedió en el sitio web de la Administración Federal de Ingresos Públicos (AFIP) en el año 2010. Puntualmente, a través de un fallo en la validación de datos, los delincuentes podían acceder al documento nacional de identidad escaneado, huella digital, fotografía y firma holográfica de cualquier contribuyente de la República Argentina.

b) Defacing

En otra categoría de ataques, uno de los más conocidos mediáticamente es el "defacement". Este ataque consiste en vulnerar un servidor web a través de distintas técnicas y modificar una o más páginas de los sitios web allí alojados. Generalmente la página modificada corresponde a la primera que visualiza el usuario al ingresar al sitio vulnerado ("index.xxx") y de esta manera se logra una rápida publicidad sobre el éxito del ataque. Esta técnica es observada en aquellos grupos que buscan enviar mensajes de protestas políticas, religiosas o institucionales, siendo los casos más conocidos y recientes, los llevados a cabo por individuos no identificados que se autodenominan "Anonymous", simplemente para ganar el reconocimiento del propio grupo.

Según el sitio Zone-h, en los últimos años ha habido una gran cantidad de ataques de defacing a sitios gubernamentales argentinos denunciados, pero se debe tener en cuenta que gran parte de los ataques nunca se denuncia, por lo que dicho número sólo debe ser tomado como un índice de referencia en relación a la verdadera cifra negra de los delitos informáticos.

30/04/2013 - Ministerio de Economía, Infraestructura y Servicios Públicos de la provincia de Salta (Figura 2). El ataque fue realizado el 30 de abril de 2013 y no fue solucionado durante varios días.

Figura 2: Ataque al sitio del Ministerio de Economía, Infraestructura y Servicios Públicos de la Provincia de Salta el 30/04/2013.

31/03/2013 - Ministerio de la Producción de la Provincia de Santa Cruz (Figura 3), captura del sitio http://zone-h.com/mirror/id/19571943.

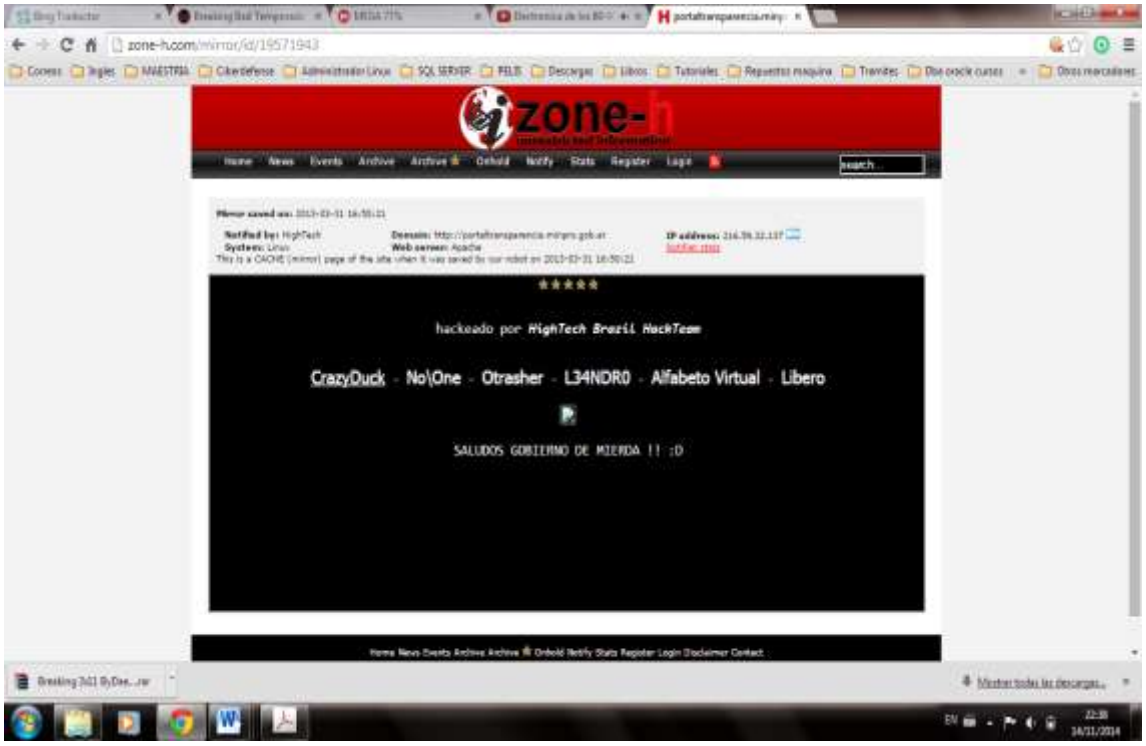

Figura 3: Ataque al sitio del Ministerio de la Producción de la Provincia de Santa Cruz el 31/03/2013.

07/01/2013 - Ministerio de Relaciones Exteriores y Culto, realizado a sus más de 50 subdominios, (Figura 4) captura del sitio http://zone-h.com/mirror/id/18899507.

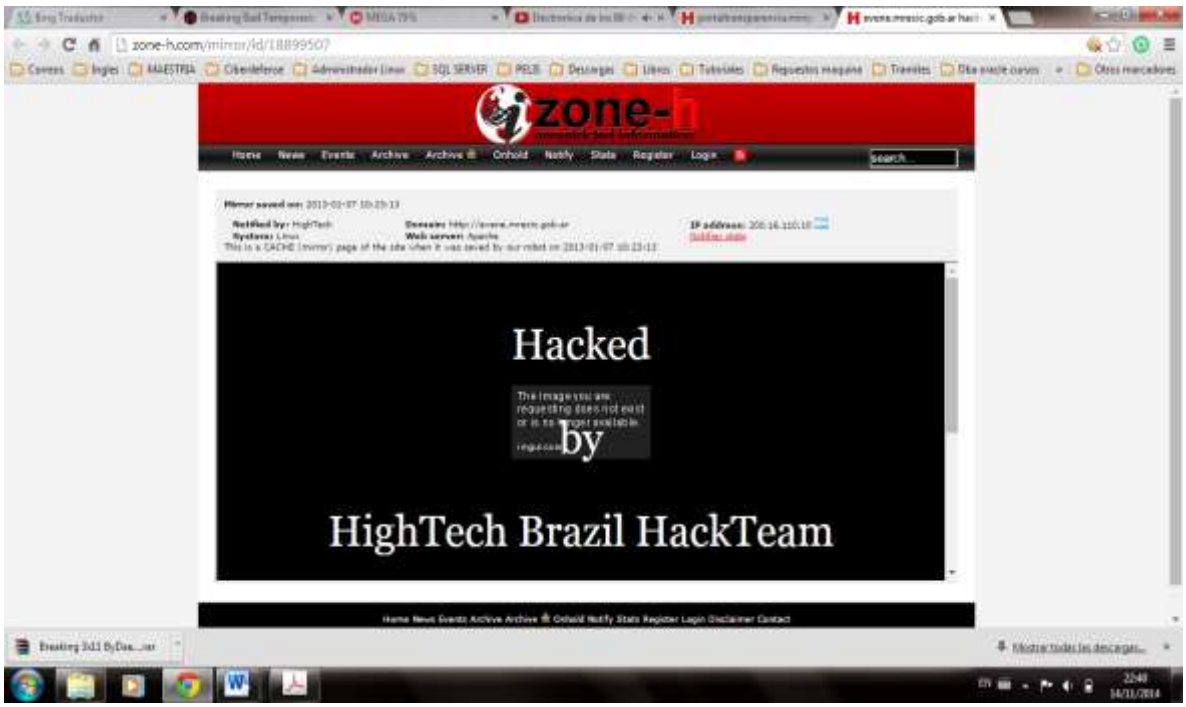

Figura 4: Ataque al sitio del Ministerio de Relaciones Exteriores y Culto el 07/01/2013.

c) Black Hat SEO7 y Watering Hole Attack

Estas técnicas, ampliamente utilizadas, están orientadas a motivos económicos y buscan posicionar en las primeros lugares de un buscador cientos o miles de sitios, mediante el uso de distintas técnicas. Las técnicas consisten en incluir un código especial (Javascript) dentro de los sitios vulnerados para lograr que, sin importar la búsqueda que realice el usuario, lo lleve a uno de estos sitios, en donde se podría resultar infectado con malware o se podrían ofrecer productos generalmente falsos o adulterados. Los servidores gubernamentales (junto a los universitarios) son muy buscados para la inserción de estos códigos porque se intenta aprovechar su reputación positiva en los buscadores, el común de las personas confía en que si el enlace es provisto por un sitio del gobierno, entonces debería ser oficial y real.

Una de las maneras de comprobar rápidamente los sitios vulnerados, es a través de la utilización de buscadores (Google, Bing, Yahoo), restringiendo los resultados a sitios gubernamentales (.GOB.AR) buscando por ejemplo ciertas drogas o productos (Figura 5):

Figura 5: Búsqueda de viagra en sitios gubernamentales argentinos el 30/04/2013.

A través de este tipo de búsquedas, cualquier atacante podrá acceder a un listado de sitios ya vulnerados, lo cual facilitará la tarea de incluir en ellos la promoción de sus productos. Cuanto mayor sea la cantidad de sitios con este tipo de códigos insertados, mayor es la publicidad y por lo tanto, más rentable se vuelve el negocio, donde la cantidad de clics es directamente proporcional a las ganancias obtenidas.

En la siguiente imagen se puede ver el código fuente del sitio web del Ministerio de Educación y cómo se realiza la redirección a la compra de productos farmacéuticos (Figura 6):

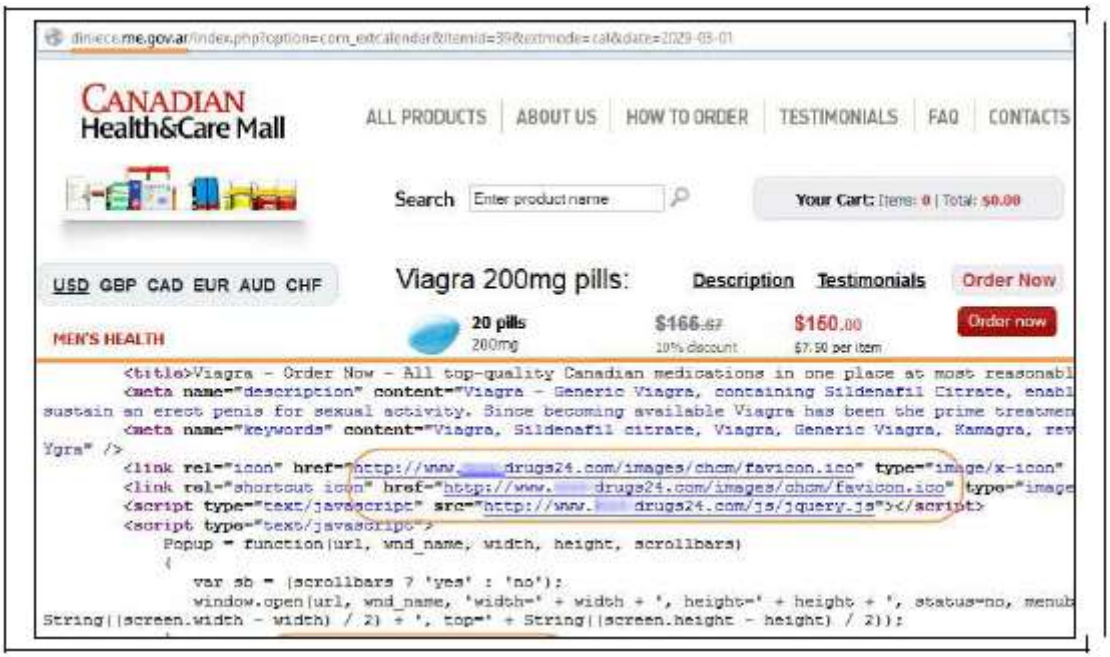

Figura 6: Sitio del Ministerio de Educación que aloja publicidad de viagra el 21/04/2013.

Similar ataque se realizó en varias páginas de un blog oficial del INTI (Instituto Nacional de Tecnología Industrial), donde incluso se ha dejado un hipervínculo expreso de "buy viagra" debajo del título de una serie de artículos científicos oficiales, vínculo que redirige a sitios que permiten comprar viagra (Figura 7:

Figura 7: Ataque al sitio del INTI (Instituto Nacional de Tecnología Industrial) modificado para alojar publicidad de viagra (28/04/2013).

d) DDoS Denegación de Servicios Distribuidos

Los ataques de Denegación de Servicio Distribuidos (DDoS) son aquellos que mediante peticiones de varios cientos o miles de dispositivos a un mismo recurso provocan la saturación del mismo y que este deje de estar disponible.

En el día 13 de Abril de 2013, desde el grupo Anonymous se llevó adelante una protesta denominada "OpFuckGobierno", en la cual en menos de 24 hs se atacaron más de 100 sitios del Gobierno Argentino, dejando a la mayoría de ellos fuera de servicio, y algunos siendo también víctimas de defacement.

Cuando un sitio es atacado inmediatamente puede apreciarse que el mismo deja de estar disponible para el resto de los usuarios. A continuación se muestran dos sitios bajo ataque (Figura 8):

Figura 8: Ataque a sitios gubernamentales el 13/04/2013.

e) Otras técnicas

También se aprovechan debilidades en las aplicaciones publicadas en los sitios web como causa de desarrollos que carecen de pruebas de seguridad y de calidad mínimas. Por ejemplo, en el caso de la (Figura 1) mostrada anteriormente, se utilizó una vulnerabilidad de Injection SQL que es un método de infiltración de código intruso que se vale de una vulnerabilidad presente en una aplicación en el nivel de validación de las entradas para realizar consultas o modificar la base de datos, en este caso la base de datos que contiene las provincias de la República Argentina (por ejemplo, Buenos Aires).

Otras técnicas que se pueden mencionar y que consisten en la modificación de un sitio web para agregar miles de enlaces con el objetivo de causar perjuicios a los usuarios son:

- Hiding Text: consiste en colocar palabras claves y enlaces en una página web, con el mismo color de fondo o dentro del código fuente, de modo que pasen desapercibidas para el usuario, pero no para el buscador.
- Spamming Keywords: técnica que implica formar frases con palabras claves (keywords) muy utilizadas, buscando mayor popularidad en la difusión.

- Keyword Stuffing: técnica que busca abusar de ciertas palabras claves dentro del contenido para hacerlas más populares, incluso no teniendo ningún tipo de relación con el contenido real del sitio o artículo.

Las técnicas mencionadas engañan a los buscadores para que al ver este sitio enlazado muchas veces, interpreten que el mismo es popular y por lo tanto deben mostrarlo en las primeras posiciones.

Ejemplo de este tipo de ataque se pudo observar en varias páginas de sitios oficiales del Gobierno de la Ciudad de Buenos Aires (Figura 9):

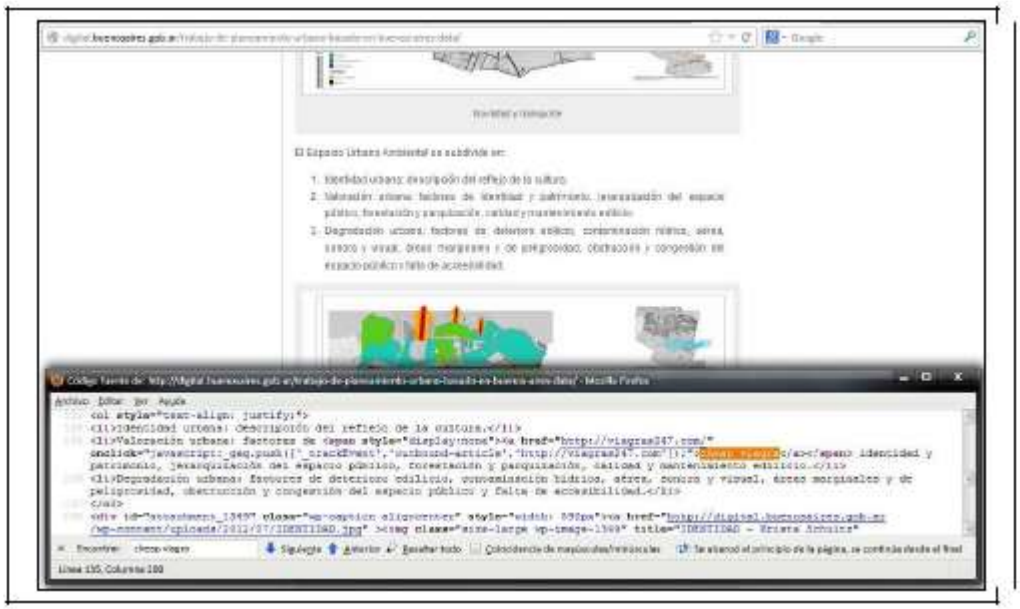

Figura 9: Publicidad oculta de viagra en el sitio del Gobierno de Buenos Aires el 28/04/2013.

Resumiendo, las técnicas utilizadas para vulnerar cualquier tipo de sitio van desde el simple acceso indebido (hacking) a través de usuarios y contraseñas débiles, hasta la utilización de intrusiones avanzadas, como la inyección de códigos maliciosos que explotan vulnerabilidades en los sistemas utilizados.

Debe tenerse en consideración que los resultados que se muestran son parte de la realidad y que la mayoría de las intrusiones producidas no son reportadas y por lo tanto pasan desapercibidas, sobre todo si persiguen objetivos económicos, dado que su anonimato favorece el hecho de que puedan permanecer en línea más tiempo y se pueden lograr mayores ingresos. Por lo tanto, es útil señalar uno de los grandes inconvenientes que tienen los delitos informáticos en Argentina, es que la cantidad real de casos ocurridos es desconocida. Es decir, en esta clase de delitos

existe una gran brecha entre la información real sobre la cantidad de casos, y aquella que realmente ha sido reportada por las víctimas, generando una cifra negra muy importante.

Hasta el momento se ha visto una importante variedad de casos que muestran los diferentes tipos de ataques que sufren las infraestructuras de los sistemas de información del gobierno argentino. Las consecuencias de dichos ataques, dependerá de varios factores, como el nivel de difusión del incidente, la popularidad del organismo o la magnitud del propio ataque. No obstante, es posible determinar sintéticamente las consecuencias más comunes:

- Daño a la imagen de la organización gubernamental afectada.
- Acceso indebido o modificación de los datos personales.
- Posible afectación de los recursos del usuario, simplemente por acceder a códigos maliciosos alojados en los sitios oficiales.
- Afectación a los derechos de protección de datos personales de los ciudadanos (casos de accesos a bases de datos).

En consecuencia, las vulnerabilidades en sitios gubernamentales existen, son muchas y variadas, y en este trabajo se trata de mostrar la realidad con fines de resaltar la importancia de la situación. Esto debe alertar especialmente a aquellos profesionales que son responsables de la seguridad de los sistemas del Estado Argentino, pero sobre todo al mismo Estado Argentino (en sentido general, en todos sus niveles de poder).

Desde el punto de vista legal, se ha observado que más allá de la necesidad de dotar a los sistemas informáticos con medidas de seguridad, en virtud de la Decisión Administrativa 669/2004, que establece que los organismos del Sector Público Nacional comprendidos en los incisos a) y c) del artículo 8º de la Ley Nº 24.156 y sus modificatorias deberán dictar o adecuar sus políticas de seguridad, conformar Comités de Seguridad en la Información y determinar funciones de los mismos y responsabilidades en relación con la seguridad. Deben existir obligaciones legales para adoptar una Política de Seguridad adecuada por cada institución y que estas respondan a una Estrategia de Ciberseguridad Nacional, sin dejar de lado la importancia de la existencia de leyes que regulen la actividad cibercriminal.

En relación a la legislación penal, se puede comprobar que todas las acciones analizadas en los casos mencionados anteriormente, se encuentran tipificadas como delitos informáticos, sin embargo, se puede estimar que pocos o ninguno de ellos ha tenido como consecuencia el

dictado de una sentencia condenatoria. A simple vista se puede observar las falencias en materia de investigación y persecución en este tipo de delitos en nuestro país y en algunos de los países mencionados en el presente trabajo, incluso en aquellos casos donde los sistemas atacados son del propio Estado.

3. POSIBLES LÍNEAS DE INVESTIGACIÓN

En este capítulo se presentan las posibles líneas de investigación identificadas a partir de la revisión literaria. Se mencionan los factores que aumentan los riesgos del ciberespacio (sección 3.1), se identifican las áreas de vacancia (sección 3.2) y se realiza la identificación del problema de investigación (sección 3.3).

3.1. FACTORES QUE AUMENTAN LOS RIESGOS DEL CIBERESPACIO

Se puede observar que existen una gran cantidad de condiciones que pueden contribuir a aumentar los riesgos en el ciberespacio. A continuación se mostraran algunas condiciones que fueron identificadas durante el desarrollo del presente trabajo:

- La industria es vulnerable. Generalmente no se está preparado para enfrentar las amenazas cibernéticas, técnicamente, organizativamente, u operativamente.
- Las amenazas se están expandiendo e intensificando.
- Las jurisdicciones legales a menudo protegen a los delincuentes y a los Estados detrás de las amenazas.
- El marco regulatorio es inconsistente, existen diferencias significativas entre los Estados.
- El nivel de conciencia de la problemática por la dirección ejecutiva de las organizaciones es demasiado bajo.
- Los gobiernos y las empresas privadas invierten muy poco presupuesto en Ciberseguridad.
- Los dispositivos móviles están creando una arquitectura de información altamente distribuida.
- Los medios sociales permiten el intercambio de datos sin precedentes.
- La ingeniería social para el acceso a la información está alcanzando nuevos niveles, cada vez más fáciles de ejecutar, debido a los medios de comunicación social.
- Muchas empresas no han calculado adecuadamente el riesgo potencial de un ciberataque.
- Muchas empresas se niegan a aceptar sus vulnerabilidades de seguridad.

3.2. IDENTIFICACIÓN DE LAS ÁREAS DE VACANCIA

Se pueden observar diferentes problemáticas en el área de Ciberseguridad de una nación, a continuación se mostrarán algunas de las más notables:

a) La vulnerabilidad de la industria: algunos estados no están preparados para resistir los ciberataques. Las regulaciones del gobierno reflejan un requisito mínimo para las empresas, en el que las obliguen a proteger la información. La mayoría de las empresas no adoptan un marco regulatorio estable para proteger sus ICIs y el nivel de conciencia es bajo, lo que las hace aún más vulnerables a los ciberataques.

b) Preparación inadecuada del Gobierno: algunos estados siguen sin impulsar programas de preparación para implementar un Sistema de Ciberseguridad Nacional. Ni siquiera están informados de forma precisa de los ataques que reciben sus ICIs. En estas condiciones es muy difícil llegar a detectar, mitigar y responder en tiempo real a las amenazas del ciberespacio.

c) Bajo nivel de conciencia: no sólo se puede observar un bajo nivel en el cumplimiento de las normas de seguridad y privacidad de la información en todos los niveles de la sociedad, sino que también hay una escasa conciencia de la necesidad de proteger la propiedad intelectual y los secretos comerciales. Muchos gobiernos no tienen programas de concientización de los ciudadanos y las empresas tampoco concientizan a los empleados sobre los peligros del uso de las nuevas tecnologías, los dispositivos móviles y medios sociales.

d) Evaluaciones inadecuadas de los riesgos: muchos estados no llevan a cabo las evaluaciones de riesgos significativas y a menudo las evaluaciones de riesgos que se llevan a cabo, son realizadas por personal que carece de suficiente perspectiva, conocimiento y experiencia. Las evaluaciones de riesgos inadecuadas pueden ser particularmente peligrosas porque infunden una falsa sensación de seguridad. Una falsa sensación de seguridad puede conducir a consecuencias devastadoras.

e) La desprotección de los datos: en la actualidad se ve cada vez más la información confidencial situada en entornos que pueden no ser seguros. A menudo la seguridad es claramente insuficiente y pocos son los controles establecidos para asegurar la integridad de la información.

f) Ataques cada vez más sofisticados: el impacto del riesgo de los ataques sofisticados es tan extenso como el alcance ilimitado de internet. El total de la población del mundo se calcula en aproximadamente 7 mil millones de personas y Cisco Systems Inc. pronostica que 50 mil millones de dispositivos móviles estarán conectados a internet para el año 2020. Esto quiere decir que existirán alrededor de siete dispositivos móviles por cada hombre, mujer y niño en el mundo. Este crecimiento exponencial implica un crecimiento directamente proporcional de los riesgos, debido a la gran distribución de datos en la nube.

g) Ausencia de una Estrategia Nacional de Ciberseguridad: el camino inicial para disponer de un ciberespacio seguro lleva a la creación e implementación de una Estrategia Nacional de Ciberseguridad que sirva como marco regulatorio y como guía para dirección, control y gestión de un Sistema de Ciberseguridad Nacional.

3.3. IDENTIFICACIÓN DEL PROBLEMA DE INVESTIGACIÓN

El presente trabajo se enfocó en la problemática de la ausencia de una Estrategia Nacional de Ciberseguridad. Y por tal motivo a continuación se enumerarán algunas de las principales características por la cual una nación no alcanza un grado aceptable de Ciberseguridad Nacional, acorde a los riesgos del ciberespacio:

a) Organizacionales

- La ausencia de un órgano de Dirección en materia de Ciberseguridad, impide la implementación de una metodología común de trabajo, que facilite la toma de decisiones, así como la coordinación e integración de todos los actores involucrados.
- La gestión desconcentrada de la Ciberseguridad Nacional, entre un conjunto de organismos de una nación.
- Los insuficientes recursos humanos, técnicos y económicos en los organismos de gestión, necesarios para implementar y gestionar las capacidades que permitan alcanzar un nivel de Ciberseguridad acorde a los riesgos del ciberespacio.

b) Operacionales

- El conocimiento parcial e insuficiente de la situación nacional en materia de Ciberseguridad, el no disponer de un estado fiable y actualizado es esencial para la toma de decisiones y la gestión de crisis en el ciberespacio.
- La ausencia de un marco de trabajo compartido en materia de Ciberseguridad. El insuficiente nivel de comunicación entre los organismos públicos relacionados con la Ciberseguridad Nacional y el sector privado se debe fundamentalmente a la ausencia de un marco de trabajo estable y abierto, que posibilite compartir de forma fluida y segura la información.
- La escasa colaboración de los sectores privados en materia de Ciberseguridad. La Ciberseguridad Nacional en la actualidad, no es un tema cerrado y exclusivo de los actores gubernamentales. Existe un gran porcentaje de las infraestructuras críticas de algunos países que están dirigidas y gestionadas por el sector privado (empresas nacionales e internacionales), por lo tanto, el aporte del sector privado al proceso de construcción de la Ciberseguridad Nacional resulta esencial.

c) Jurídicas

- La ausencia de normativa específica y completa en materia de Ciberseguridad. No existe legislación desarrollada que permita regular los delitos cibernéticos en el ámbito nacional e internacional y que permita la aplicación de la ley en el ámbito de la ciberseguridad.

d) Políticas

- La ausencia de políticas que fomenten la colaboración público-privada en materia de Ciberseguridad, es una de las mayores dificultades para alcanzar un nivel de seguridad acorde.
- La ausencia de una política estatal en materia de concientización y educación. Cabe destacar que muchos países están desarrollando políticas en materia de concientización como eje fundamental para la creación de una cultura de Ciberseguridad. En este caso, cabe destacar una doble misión, por un lado, concientizar y educar al conjunto de la ciudadanía sobre los riesgos del ciberespacio, y por otro lado, identificar futuros talentos en el campo de la Ciberseguridad dentro de la comunidad escolar y universitaria.

4. CONCLUSIÓN

A escala global cada país aborda de manera distinta la Ciberseguridad, dependiendo de su panorama económico, político y cultural imperante. Algunos países consideran la Ciberseguridad principalmente como un asunto de seguridad nacional y defensa. Otros opinan que tiene un mayor impacto en el desarrollo económico o en la competitividad internacional. Otros más la ven como un factor clave para la educación, la interacción social y el bienestar de los ciudadanos, aunque sabiamente muchos países están tratando de incorporar todas estas consideraciones en sus Estrategias Nacionales de Ciberseguridad.

A pesar de la variedad de enfoques, están surgiendo estudios de casos que ayudarán más eficientemente a todos los países a mejorar sus Estrategias o Políticas de Ciberseguridad. Muchos gobiernos obtienen avances tecnológicos rápidos pero tienen que lidiar con burocracias que se interponen en su camino, lo que facilita a los hackers vías ilícitas para operar sin preocuparse mucho por ser perseguidos o capturados. Uno de los principales impedimentos para frenar las actividades cibernéticas ilícitas en los últimos años fue la falta de legislación adecuada y políticas robustas de Ciberseguridad, conjuntamente con la falta de experiencia de los investigadores en delincuencia cibernética y la escasez de fiscales especializados en delitos relacionados con las tecnologías de información. Muchos países están encontrando dificultades para frenar y procesar judicialmente a los hackers y a otros delincuentes cibernéticos.

Así también se puede observar la necesidad de profesionales altamente capacitados que puedan asegurar las redes, diagnosticar intrusiones y manejar eficazmente los incidentes cibernéticos. Este problema se manifiesta mayormente en Latinoamérica, debido a las bajas tasas de matrículas en programas de formación técnica. Dado el tiempo que se requiere para adquirir habilidades y experiencia práctica en Ciberseguridad, esta tasa baja de matrículas podría tener un impacto negativo en los próximos años.

A nivel local en nuestro país, se puede apreciar en este trabajo un pequeño espectro en lo que se refiere a la Ciberseguridad, ya que solo se pudieron mostrar las vulnerabilidades de los sitios gubernamentales, y esto solo es una pequeña parte en lo que se refiere a la Ciberseguridad, no se tuvieron en cuenta vulnerabilidades de sitios web privados, redes públicas y privadas, servicios informáticos empresariales, infraestructuras críticas de información ICIs, computadoras personales, entre otras.

Las vulnerabilidades mencionadas son en definitiva consecuencias de la falta de implementación de una Estrategia Nacional de Ciberseguridad que establezca los lineamientos y un marco jurídico sostenible para implementar un Sistema de Ciberseguridad a nivel nacional acorde a los riesgos actuales del ciberespacio.

Se puede observar que una Estrategia Nacional de Ciberseguridad debe ser un instrumento que guíe a los responsables de la dirección y gestión de la Ciberseguridad Nacional y que involucre a todas las organizaciones públicas o privadas y a la sociedad para trabajar en coordinación, además debe servir como instrumento que contribuye a la defensa y debe definir una visión estratégica basada en los siguientes pilares:

a) Responsabilidad

La seguridad del ciberespacio nacional es responsabilidad del gobierno, este debe asumir el liderazgo, para ello, deberá crear un Sistema Nacional de Ciberseguridad. Se deberá propiciar la participación no solo de los actores gubernamentales tradicionales, sino también de los actores privados, comunidad universitaria, asociaciones, expertos, y representantes de la ciudadanía.

b) Política

El Gobierno debe mostrar una determinación política para hacer frente a los riesgos y amenazas cibernéticas y, para ello deberá fijar objetivos y prioridades. La creación de un Sistema de Ciberseguridad Nacional permitirá reducir los riesgos de que cada organismo involucrado decida sus propias líneas de actuación, debiendo actuar en coordinación y bajo un marco regulatorio estable. Asimismo esta política deberá fomentar las relaciones internacionales.

5. REFERENCIAS

5.1. ARTÍCULOS

Acosta, O., Rodriguez, J., Arnáiz de la Torre, D., & Taboso Ballesteros, P. (2009). Seguridad nacional y ciberdefensa (1a. ed.). Madrid: Fundación Rogelio Segovia para el Desarrollo de las Telecomunicaciones.

Borghello, C., & Temperini, M. (2013). Ciberseguridad Nacional Argentina: Cracking de Servidores de la Administración Pública. Simposio de Informática y Derecho. Jornadas Argentinas De Informática, Nº 42.

de Europa, C. (2001). Convenio sobre la Ciberdelincuencia. European Treaty Series, (185).

Fojón Chamorro, E., Coz Fernández, J., Miralles López, R., & Linares Fernández, S. (2014). La Ciberseguridad Nacional un compromiso de todos. Jornada Internacional De Seguridad De La Información, N° 16.

Holt, M. W. (2014). Aligning National Cyber Security Strategies to International Guidance: A First Step Toward Improving Incident Response Capabilities Across NATO. Best Practices in Computer Network Defense: Incident Detection and Response, 35, 65.

Insulza, J. (2013, May 20). OAS and Trend Micro Report Examines Cybersecurity Trends in the Americas. Bioterrorism Week.

Joyanes Aguilar, L. (2010). Ciberseguridad: Retos y amenazas a la seguridad nacional en el ciberespacio. Madrid: Ministerio de Defensa.

Kruidhof, O. (2014). Evolution of National and Corporate CERTs–Trust, the Key Factor. Best Practices in Computer Network Defense: Incident Detection and Response, 35, 81.

Luiijf, E., Besseling, K., & De Graaf, P. (2013). Nineteen National Cyber Security Strategies. International journal of critical infrastructures, 9(1), 3-31.

Sullivan, B. (2014, May 28). OAS and Symantec to Present Cyber Security Report on June 2nd. States News Service.

5.2. DOCUMENTOS WEB

Ciberdelincuencia.Org. Fuentes de Información.
http://ciberdelincuencia.org/fuentes/legislacion.php.
Página vigente al 20/01/2015.

CICTE (COMITÉ INTERAMERICANO CONTRA EL TERRORISMO). FORTALECIMIENTO DE LA SEGURIDAD CIBERNÉTICA EN LAS AMÉRICAS.
http://www.cicte.oas.org/rev/en/Documents/Declarations/DEC%201%20rev%201%20DECLARACION%20CICTE00749S04.pdf
Página vigente al 20/01/2015.

Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación (2011). LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA. Bogotá: Colombia.
http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf
Página vigente al 20/01/2015.

Departamento de Segurança da Informação e Comunicações (2010). LIVRO VERDE SEGURANÇA CIBERNÉTICA NO BRASIL. Brasília: PRESIDÊNCIA DA REPÚBLICA.
http://dsic.planalto.gov.br/documentos/publicacoes/1_Livro_Verde_SEG_CIBER.pdf
Página vigente al 20/01/2015.

Departamento de Seguridad Nacional de la Presidencia del Gobierno (2013). ESTRATEGIA DE CIBERSEGURIDAD NACIONAL. Palacio de la Moncloa: España.
http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/ES_NCSS.pdf
Página vigente al 20/01/2015.

Department of Defense (2011). Department of Defense strategy for operating in cyberspace. Washington, D.C.: United States.
http://www.defense.gov/news/d20110714cyber.pdf

Página vigente al 20/01/2015.

ENISA (European Union Agency for Network and Information Security). National Cyber Security Strategys (NCSSs). National Cyber Security Strategies in the World.
http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world.
Página vigente al 20/01/2015.

European Network and Information Security Agency (ENISA), 2012. National Cyber Security Strategies - Setting the course for national efforts to strengthen security in cyberspace. Resilience and CIIP Program at ENISA.
http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper/at_download/fullReport
Página vigente al 20/01/2015.

Federal Ministry of the Interior (2012). Cyber security strategy for Germany. Berlin: Germany.
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile
Página vigente al 20/01/2015.

Information Security Policy Council (2013). Cyber Security Strategy Towards a world leading resilient and vigorous cyberspace. National Centre of Incident readiness and Strategy of Cybersecurity. Government of Japan.
http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf
Página vigente al 20/01/2012.

Levin, A., Goodrick, P., & Ilkina, D. (2013). Securing Cyberspace: A comparative review of strategies worldwide. The 2014 IT Canadian Conference.
http://www.ryerson.ca/tedrogersschool/privacy/documents/Ryerson_cyber_crime_final_report.pdf
Página vigente al 20/01/2015.

Minister for the Cabinet Office (2011). The UK Cyber Security Strategy Protecting and promoting the UK in a digital world. London: Government of United Kingdom.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

Página vigente al 20/01/2015.

Minister of Public Safety (2010). Canada's cyber security strategy: For a stronger and more prosperous Canada. Ottawa: Government of Canada.
http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx
Página vigente al 20/01/2015.

Ministry of Economic Affairs and Communication (2014). Cyber Security Strategy 2014 - 2017. Republic of Estonia.
https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf
Página vigente al 20/01/2015.

Ministry of Foreign Affairs of the Russian Federation (2000). INFORMATION SECURITY DOCTRINE OF THE RUSSIAN FEDERATION. President of the Russian Federation. http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument
Página vigente al 20/01/2015.

OEA (Organización de Estados Americanos). UNA ESTRATEGIA INTERAMERICANA INTEGRAL DE SEGURIDAD CIBERNÉTICA.
http://www.oas.org/juridico/english/cyb_pry_estrategia.pdf
Página vigente al 20/01/2015.

Secretary General for Defence and National Security (2011). France's strategy Information systems defence and security. Agence nationale de la sécurité des systèmes d'information France. http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf
Página 20/01/2015.

Zone-h. Archive.
http://zone-h.com/archive/special=1.
Página vigente al 20/01/2015.