ESCUELA SUPERIOR DE GUERRA NAVAL

CENTRO DE ESTUDIOS ESTRATÉGICOS Y MARÍTIMOS

Ciberseguridad Nacional

por
Contralmirante Oscar Anderson Machado

Contralmirante Santiago LLOP Meseguer
Presidente del Centro de Estudios Estratégicos y Marítimos

2014

INFORME DE DISCUSIÓN

N° 002/2014 – CIAEM

CIBERSEGURIDAD NACIONAL

---

1. Generalidades

"*La guerra actual puede desencadenarse desde un café o restaurante*". La ciberguerra es fragmentada y compleja, en algunos sentidos más que la convencional. Nos referimos al quinto dominio de la guerra, junto a los ya tradicionales de tierra, mar, aire y espacio.

La seguridad nacional debe proteger y corregir las vulnerabilidades de nuestros activos patrios, en lo que se refiere a la CIBERSEGURIDAD. Las agresiones no siempre serán exclusivamente cibernéticas. Por ejemplo, una agresión militar convencional podría venir acompañada -en el antes, durante o el después- de un ciberataque. Y al revés: un ciberataque militar podría venir acompañado de acciones más convencionales. Ante toda agresión, cada vulnerabilidad es un talón de Aquiles del activo, es uno de sus puntos más débiles. No hay un activo sin vulnerabilidades, ni existe activo al que no se le pueda dañar.

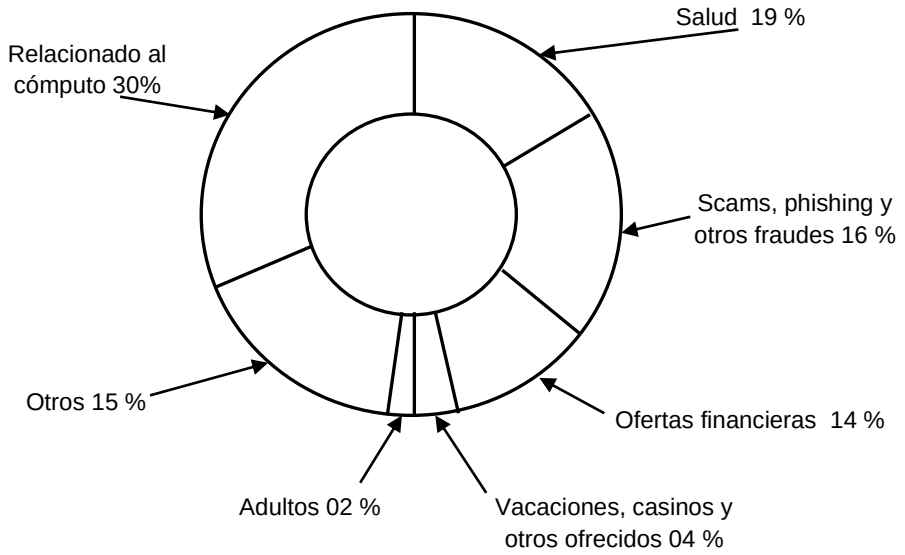
El ciberespacio es un nuevo ámbito de relación que ha proporcionado el desarrollo de las nuevas tecnologías de la información y las comunicaciones, pero que también ha diluido fronteras, permitiendo una globalización sin precedentes, que propicia nuevas oportunidades, pero conlleva serios riesgos y amenazas.

La creciente dependencia de la sociedad del ciberespacio y su fácil accesibilidad hacen que cada vez sean más comunes y preocupantes las intromisiones en este ámbito. En buena medida, el ciberespacio es un medio para la materialización de otros riesgos y amenazas. En el año 2011, se produjo el mayor número de amenazas descubiertas, estimándose en 70 millones de programas malware circulando por todo el mundo y los teléfonos inteligentes (smartphones) se han convertido en el principal medio de su difusión.

El 70% de los correos electrónicos son spam y los ciberataques en sus diversas modalidades como ciberterrorismo, ciberdelito, ciberespionaje o activismo en la red, se han convertido en un potente instrumento de agresión contra las redes eléctricas inteligentes, la computación en nube, las redes de automatización industrial, los sistemas de transporte inteligentes, la ciberadministración, sistemas y componentes de la defensa nacional y la banca electrónica, entre otros tipos de infraestructura. La falla de uno de estos sistemas afecta a los demás. La mayor facilidad de conexión y la mayor eficacia en las comunicaciones trae consigo una mayor vulnerabilidad frente a los ciberataques. (CMTI, 2012, p.1).

El presidente Barack Obama, ha señalado que las pérdidas debido a los crímenes cibernéticos en el año 2011 ascienden a Un Trillón de Dólares, todo un submundo, mucho mayor al de las drogas aunque la suma sea cuestionable, sin embargo, sólo el 2008, la compañía de telefonía VERIZON reportó el hurto de 285 millones de registros personales, incluyendo los detalles de tarjetas de crédito y cuentas bancarias.

Categorías de Spam Global en % correspondiente a mayo de 2010



Fuente Symantec

El recurso de la ciberguerra constituye un recurso atractivo para los actores que buscan estrategias asimétricas de enfrentamiento contra adversarios más poderosos en el terreno de las armas, ya que como se ha dicho, no existen fronteras ni se requiere encontrarse físicamente en el objetivo para materializar el atentado. Para ubicarnos en el terreno en el cual se desenvuelve la ciberguerra, debemos entender que el ciberespacio es un entorno creado por el hombre y que está compuesto por tres (3) niveles:

a. **Físico**, es aquel compuesto por la infraestructura y equipamientos informáticos que soportan los sistemas de información.

b. **Sintáctico**, correspondiente a las instrucciones y configuraciones básicas introducidas por los diseñadores y usuarios de los equipos de informática. En este nivel actúan los hackers.

c. **Semántico**, abarca la información que el equipo contiene lo que incluye datos, programas y códigos que permiten al ordenador efectuar determinadas funciones.

El bajo coste y mínimo riesgo que suponen para el atacante y su fácil empleo, efectividad y accesibilidad, son factores que explican la extensión del fenómeno. El anonimato que ofrece Internet hace que sea relativamente fácil ocultar la identidad de uno y por lo tanto, a veces es difícil determinar si el autor del delito cibernético es un individuo, una organización o un agente de un tercer actor (ya sea estatal o no estatal).

Riesgos y Amenazas a la CIBERSEGURIDAD Nacional

Gráfico N°1. Estrategia de CIBERSEGURIDAD Nacional. Dpto de Seguridad Nacional, Presidencia de Gobierno (2013).

Sin embargo, aún no existe una definición aceptada en todo el mundo ni estándares de seguridad de cumplimiento obligatorio. Este vacío obstaculiza los esfuerzos de protección que deben emprenderse a nivel nacional e internacional toda vez que las redes y sistemas informáticos tienen hoy un carácter transfronterizo.

Existe la posibilidad de que un estado posea los medios físicos y humanos para iniciar una agresión cibernética contra otro estado, pero también, es posible que este estado no posea total inmunidad contra una ciber represalia, como por ejemplo es el caso de Corea del Norte. Existen otros ejemplos de ciberataques en los cuales se puede inferir la "identidad" de los autores pero no se puede afirmar con total seguridad su autoría. Tal es el caso de los siguientes ejemplos:

1) En junio de 1982 un satélite de alarma temprana americano detectó una gran explosión en Siberia, aparentemente se había producido una explosión en el gasoducto ruso a consecuencia de un mal funcionamiento del sistema de válvulas de control computarizado. Esta explosión se produjo como consecuencia de la infiltración en el software de control, presumiblemente por parte de la CIA, quienes sembraron una bomba lógica lo que originó sobrepresiones en las bombas que excedían largamente las tolerancias en las soldaduras y juntas. Esto porque se determinó que el programa había sido robado por espías rusos a una empresa canadiense.

2) A China se le acusa de atacar frecuentemente los ordenadores de los principales contratistas occidentales comprometidos en la construcción del caza F-35, futuro pilar del poder aéreo norteamericano.

3) Año 2007 se produjo la Primera Guerra en la Red WWI (Web War 1), ésta fue un "ataque concertado de negación" en el que se interrumpieron los servicios al estado de Estonia, a sus medios y los bancos, esto como consecuencia a la decisión de mudar de sitio un memorial de guerra soviético ubicado en el centro de la ciudad de Tallinn. Esta agresión obligó al estado de Estonia a cortar su servicio de internet.

4) En 2008, durante el ataque ruso sobre Georgia, se produjo un ataque aún más devastador, en el que se pudo apreciar la coordinación entre el ataque cibernético y el avance de las columnas militares rusas. Las páginas del gobierno y las de los medios se "cayeron", las líneas telefónicas fueron disturbadas complicando la capacidad de Georgia de dar a conocer los hechos al exterior.

5) El gusano STUXNET es una aplicación que infecta los sistemas de control industrial de una manera peculiar, se trata de un misil cibernético que explota las debilidades del sistema operativo Windows de Microsoft pero que a la vez resalta la potencialidad de las armas cibernéticas que actúan puntualmente sobre los sistemas del blanco. Este misil fue detectado en Alemania y en la planta nuclear iraní de Bushehr dónde no se ocasionaron daños, sin embargo, en la refinería nuclear de Natanz las centrifugadoras dejaron de funcionar correctamente y aunque no se paralizaron, la desaceleración logró retrasar el proyecto nuclear iraní, lo que demuestra que los blancos eran estas bombas centrífugas.

6) En 2008, el representante de Huawei, firma china, en Gran Bretaña, uno de los grandes contratistas en telefonía, recibió la buena pro para modernizar el sistema telefónico británico por la suma de USD 14 Mil Millones de Dólares. El jefe, Ren Zhengfei, fue identificado por el servicio secreto británico como un ex oficial del ejército chino, hecho que causó revuelo toda vez que estaría en condiciones de tender redes y líneas a estamentos del gobierno con la posibilidad de sembrar "puertas falsas" lo que permitiría a los chinos evadir con facilidad los sistemas de detección y obtener información sensible para su explotación.

7) El 14 de mayo de 2014, se hace pública la decisión del gobierno de Estados Unidos de iniciar un proceso judicial por ciberespionaje contra cinco oficiales del ejército de China, a quienes se acusa de robar secretos de la industria siderúrgica norteamericanos para ayudar a empresas estatales chinas.

2. Situación Nacional de CIBERSEGURIDAD en los Estados Unidos de América

El presidente Obama declaró de interés nacional estratégico la infraestructura digital de América y designó al Sr. Howard Schmidt, ex gerente de seguridad de Microsoft, como Zar encargado de la CIBERSEGURIDAD. En mayo de 2010, el pentágono estableció su nuevo Puesto de Comando Cibernético (Cybercom) a cargo del General Keith Alexander director de la Agencia de Seguridad Nacional (NSA) quien recibió la orden de asumir funciones en todo el espectro a fin de defender las redes militares americanas y atacar las de otras naciones.

Otro hecho de importancia fue el que reportó la Guardia Civil española en marzo de 2010, cuando tras un paciente seguimiento logró desmantelar una de las mayores redes de computadoras "ZOMBIES" (Denominación con la que se asigna a computadores personales que tras haber sido infectados por algún tipo de malware, pueden ser utilizadas por terceros para ejecutar actividades hostiles.

Este uso se produce sin la autorización o el conocimiento del usuario del equipo) conocida como “BotNet Mariposa” conformada por más de 13 millones de direcciones IP infectadas y distribuidas en 190 países alrededor del mundo. En el siguiente cuadro se muestra el porcentaje de máquinas infectadas correspondiente a cada país:

N°	País	%	N°	País	%
1	India	19.14	11	Perú	2.42
2	México	12.85	12	Irán	2.07
3	Brasil	7.74	13	Arabia Saudita	1.85
4	Corea	7.24	14	Chile	1.74
5	Colombia	4.94	15	Kazakhstan	1.38
6	Rusia	3.14	16	Emiratos Arabes	1.15
7	Egipto	2.99	17	Marruecos	1.13.
8	Malasia	2.86	18	Argentina	1.10
9	Ucrania	2.69	19	Estados Unidos	1.05
10	Paquistán	2.55			

TABLA de países Latinoamericanos más afectados por una red de Zombies en marzo 2010
Fuente: www.infospyware.com

De lo anteriormente expuesto, se desprende la importancia directa e implícita que tiene la CIBERSEGURIDAD para todos los países y estados responsables, más aún, cuando el acceso limitado o nulo a Internet así como el analfabetismo digital constituyen una gran desventaja para el desarrollo de la población y del estado. Todos deben tener la capacidad de acceder al ciberespacio así como a un flujo continuo y seguro de la información, por lo que el estado debe garantizar la integridad y seguridad del acceso.

Así tenemos que la seguridad de la información debe preservar, la confidencialidad (que la información no sea divulgada a terceros), la integridad (la información debe ser exacta y completa) y la disponibilidad de la información (debe estar disponible para el usuario al momento que éste la necesite).

Los ilícitos provienen cada vez con más frecuencia de grupos terroristas, redes de crimen organizado, empresas, estados o individuos aislados. La CIBERSEGURIDAD también puede comprometerse por causas técnicas o fenómenos naturales.

La ausencia de una legislación armonizada en la materia de CIBERSEGURIDAD, así como el hecho de que internet fue diseñado como un canal accesible, sencillo y útil, sin considerar la dimensión de su seguridad, son elementos que incrementan las posibilidades de que las ciberamenazas se materialicen en el Perú. Por anexo se presenta el listado de normas técnicas existentes relativas al tema.

El Perú, aun cuando está gozando de un auge económico sin precedentes en su historia, también está sufriendo una escalada en la incidencia de los delitos económicos, convirtiéndose éstos en un problema serio para el país. Sólo en los últimos 24 meses, una de cada cinco compañías ha sido víctima de alguna modalidad de delito económico, siendo los más agudos los cibernéticos.

Un estudio de la Cámara de Comercio de Lima, publicado este año, señala que más de la mitad de las empresas han aumentado sus gastos en los últimos cinco años, específicamente en el área de la seguridad. Una de cada diez empresas destina el cinco por ciento de su presupuesto a gastos de seguridad electrónica preventiva contra el delito. Una cifra general revelada en el año 2010, estimaba que el gasto en seguridad ascendía a 71 mil millones de soles, lo que equivale al 20% del PBI

A nivel estatal, no se cuenta con una entidad rectora que norme y centralice los esfuerzos en la lucha contra los ciberataques y el Perú se encuentra a la zaga tal como se demuestra en las siguientes dos tablas. En el entorno privado, los esfuerzos son aislados y proporcionales con la magnitud e importancia de la empresa en cuestión. Por su parte, las entidades del estado no están organizadas para enfrentar la amenaza cibernética y cada una administra sus recursos conforme a la preparación y experiencia de su personal, concordante con los recursos disponibles, hecho que se traduce en una falta de estandarización de los medios e incapacidad para una posterior articulación de los sistemas informáticos que permitan el intercambio de información vital a través de medios seguros.

Estados con doctrina militar y organizaciones para la CIBERSEGURIDAD y Ciberguerra

Albania	Corea Norte	Irán
Alemania	Corea Sur	Italia
Argentina	Dinamarca	Kazajistán
Austria	Estados Unidos	Malasia
Australia	Estonia	Noruega
Bielorusia	Finlandia	Reino Unido
Birmania	Francia	Polonia
Brasil	Georgia	Rusia
Canadá	Holanda	Suiza
China	India	Turquía
Colombia	Israel	Ucrania

Estados con Políticas y Organizaciones para la CIBERSEGURIDAD

Ant. y Barbuda	Hungría	Nigeria
Bélgica	Indonesia	Omán
Brunéi	Japón	Pakistán
Bulgaria	Jordania	Portugal
Croacia	Kenia	Rep. Checa
Cuba	Letonia	Serbia
Chipre	Lituania	Singapur
Eslovaquia	Luxemburgo	Sudáfrica
Eslovenia	Maldivas	Suecia
España	Malta	Emiratos Árabes Unidos
Filipinas	Marruecos	Vietnam
Ghana	Nueva Zelanda	Zimbabue

Los ciberataques no solo generan costos económicos elevados, sino que también, y lo que es más importante, ocasionan la pérdida de confianza de los ciudadanos en unos sistemas que en la actualidad resultan críticos para el normal funcionamiento de la sociedad y de la seguridad nacional. Un hipotético ataque a la banca afectaría financieramente al sistema con transacciones ilícitas automatizadas con severo impacto en la tributación y el origen ilícito de los fondos.

La Policía Nacional cuenta con una limitada unidad, dedicada a investigar y contrarrestar los ilícitos cibernéticos, mientras que las Fuerzas Armadas con escasos recursos humanos y materiales, efectúan modestos esfuerzos para evitar la penetración y sustracción de información sensible a la seguridad nacional, lo que aunado a la ausencia de normas legislativas y la escasa cultura de seguridad del público en general figuran como las principales causas a la falta de seguridad cibernética. Esto explica los intentos de ataque registrados contra infraestructuras gubernamentales. De perpetrarse en las redes del gobierno, las entidades del estado serían afectadas con la sustracción de información sensible a la seguridad interna y externa.

3. Conclusiones

Para hacer frente a estas ciberamenazas y buscando anticiparnos a las del futuro, es necesario considerar la creación de un organismo nacional rector de las normas y procedimientos de CIBERSEGURIDAD en el Perú. Este organismo deberá tener una estructura orgánica que responda a la visión integral con objeto de dar respuesta conjunta y adecuada para preservar la CIBERSEGURIDAD.

La estructura orgánica podría estar conformada, por ejemplo, por siete órganos de línea, a cargo de un Coordinador de Seguridad Nacional, bajo la dirección del Presidente del Consejo de Seguridad Nacional.

La dirección de Coordinación de Seguridad Nacional, deberá ser una entidad nueva, a cargo del Ministerio de Defensa y dotada con personal con experiencia en el ámbito de la guerra electrónica y CIBERSEGURIDAD. Será el responsable ante el Presidente del Consejo de Seguridad Nacional de coordinar la Política de Seguridad Nacional en el ámbito del ciberespacio.

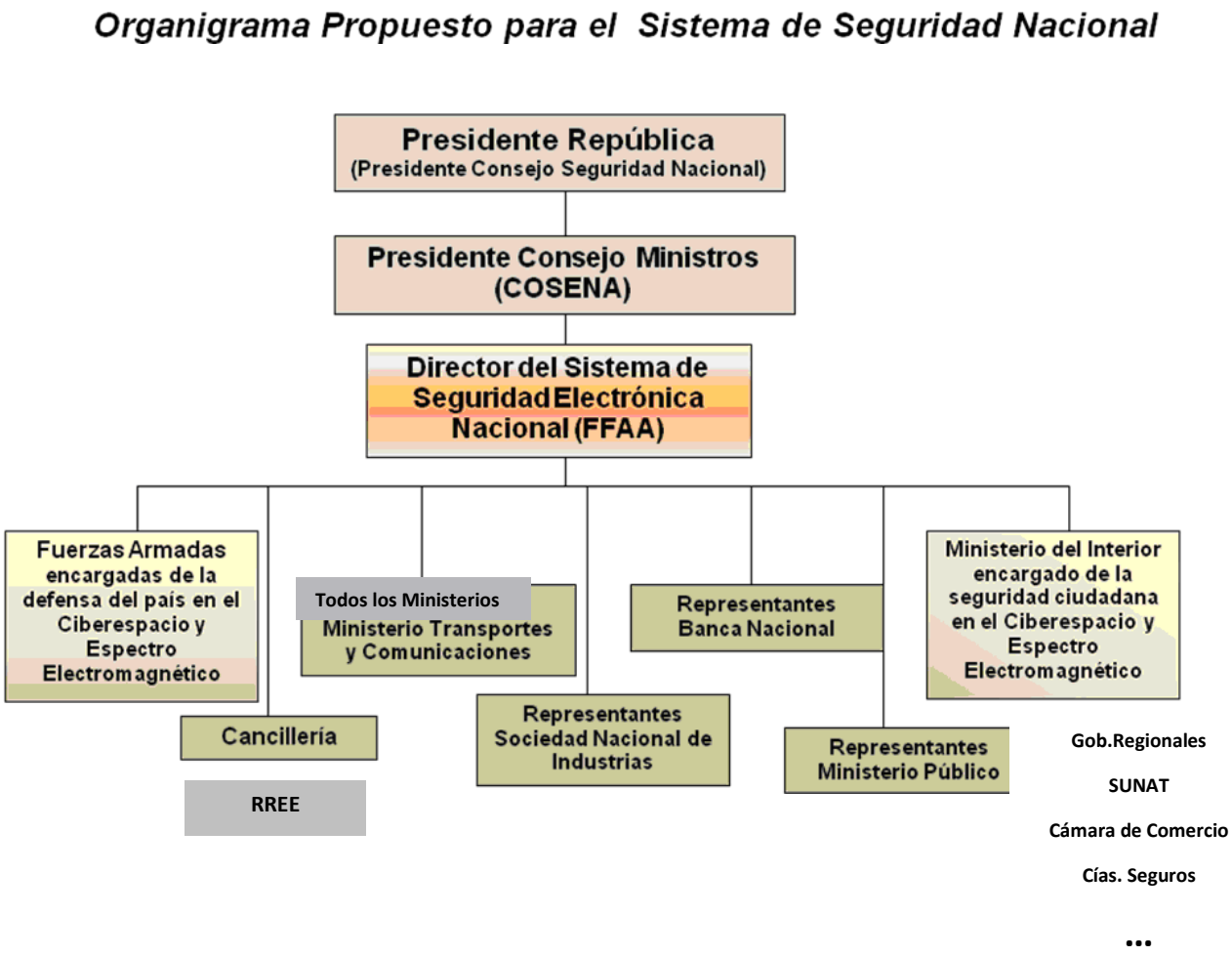


Fig. 2. Proyecto de Organigrama del Sistema de Seguridad Nacional

Además, se encargaría de reforzar las relaciones de coordinación, colaboración y cooperación entre las distintas administraciones públicas con competencias en materia de CIBERSEGURIDAD, así como entre los sectores públicos y privados, facilitando la toma de decisiones del propio Consejo mediante análisis, estudio y propuesta de iniciativas tanto en el ámbito nacional como en el internacional.

Definirá un ámbito de actuación con sus objetivos y respectivas líneas de acción estratégicas.

N°	Línea de acción
1	Capacidad de prevención, detección, respuesta y recuperación ante las ciberamenazas.
2	Seguridad de los sistemas de información y telecomunicaciones que soportan la administración pública.
3	Seguridad de los sistemas de información y telecomunicaciones que soportan las infraestructuras críticas.
4	Capacidad de investigación y persecución del ciberterrorismo y la ciberdelincuencia.
5	Seguridad y resiliencia de las TIC en el sector privado.
6	Conocimientos, competencias e I+D.
7	Cultura de CIBERSEGURIDAD.
8	Compromiso Internacional.

En el ámbito de la CIBERSEGURIDAD, tendrá como objetivo el de garantizar el uso seguro de las redes y de los sistemas de información a través del fortalecimiento de las capacidades propias de prevención, detección y respuesta a los ciberataques. Este objetivo, podría ser alcanzado a través de ocho líneas de acción, las que enmarcarían las actuaciones concretas para la preservación de la CIBERSEGURIDAD Nacional, como se propone a continuación: (Ibid, p.5)

Con la finalidad de articular los esfuerzos aislados, principalmente en los sectores de Defensa, Interior, Industria, Servicios Públicos Esenciales, Comunicaciones, Banca, Justicia, Ministerio Público, Economía y Finanzas; el ente rector de la CIBERSEGURIDAD tendría como finalidad la coordinación de los esfuerzos a fin de asegurar la interoperatibilidad de los sistemas, para garantizar la protección de los sistemas y la resiliencia de los servicios de la Administración Pública y las infraestructuras críticas de forma tal, que se brinde una garantía relativa que el país continuará funcionando a pesar de los ataques deliberados o accidentales que ocurran. (Documento de Análisis 65; 2013, p 5,6).

Así mismo, el ente rector deberá velar por la disponibilidad de productos confiables, de línea técnica preferentemente estandarizada, para lo que será necesario potenciar, impulsar y reforzar las capacidades nacionales de investigación y desarrollo en CIBERSEGURIDAD de las Tecnologías de la Información y Comunicaciones (TIC).

4. Recomendaciones

Que el Ministerio de Defensa considere tomar las siguientes acciones iniciales en coordinación con la Presidencia del Consejo de Ministros, con el Ministerio de Economía y con el Ministerio del Interior:

a. Formar la Dirección de Coordinación de Seguridad Nacional en el entorno del Ministerio de Defensa. (Por ser su personal integrante formado con el criterio de seguridad.) la misma que deberá:

1) Implementar instancias apropiadas para prevenir, atender, controlar y generar recomendaciones que regulen los incidentes y/o emergencias cibernéticas para proteger la infraestructura crítica nacional;

2) Diseñar y ejecutar planes de capacitación especializada en CIBERSEGURIDAD y ciberdefensa; y

3) Fortalecer el cuerpo normativo y de cumplimiento en la materia.

b. Contratar cursos de capacitación e instrucción inicial en el país o en el extranjero, para ser dictado al personal de dotación de la Dirección de Coordinación de Seguridad Nacional por personal altamente capacitado y experimentado (Por ejemplo de USA, Alemania, España, Colombia).

c. Recomendar la adecuación de las leyes para que se considere en éstas las nuevas amenazas y puedan así ser juzgados y sancionados los infractores.

d. Asignar los medios económicos necesarios a la Dirección de Coordinación de Seguridad Nacional para que pueda adquirir el equipamiento de control, fiscalización e intervención necesario.

e. Asignar el control y la seguridad del dominio ***.mil*** a la Fuerza Armada, el dominio del gobierno ***.gob*** y el corporativo ***.com*** al Ministerio del Interior y de las compañías proveedoras de servicios de internet respectivamente.

f. Nombrar una comisión para que se encargue de:

1) Establecer los lineamientos de política para el desarrollo e impulso de la estrategia de CIBERSEGURIDAD y Ciberdefensa.

2) Emitir los lineamientos de seguridad en el Ciberespacio que minimicen el nivel de riesgo al que las entidades están expuestas.

3) Identificar la estructura crítica Nacional.

g. Sostener reuniones periódicas con los representantes de los siguientes sectores, los que deberán designar un representante de sus respectivas instituciones, así como crear la oficina de Coordinación de Seguridad adscritas a la Dirección de Coordinación de Seguridad Nacional, a fin de verificar el avance en los diferentes compromisos y responsabilidades asignadas:

1) Ministerio Público, Poder Judicial

2) Ministerio de Defensa, Ministerio Interior, Ministerio Relaciones Exteriores

3) Todos los Ministerios, Embajadas

4) Superintendencia de Banca y Seguros, compañías de seguros

5) SUNAT

6) Sociedad Nacional de Industria, Cámara de Comercio

7) Gobiernos Regionales

8) Marina de Guerra del Perú,

9) Fuerza Aérea del Perú, y

10) Policía Nacional del Perú.

GLOSARIO BÁSICO DE TÉRMINOS

Amenaza: Violación potencial de la seguridad. (Rec. UIT-T X.800, 3.3.55)

Amenaza informática: La aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado.

Ataque cibernético: Acción organizada y/o premeditada de una o más personas para causar daño o problemas a un sistema informático a través del ciberespacio.

BotNet: Es el nombre que se le da a una red de ordenadores que combina sus recursos para realizar una tarea común repartiendo la carga de trabajo entre todos los ordenadores (FireEye, 2014).

CERT: (Computer Emergency Response Team) Equipo de Respuesta a Emergencias cibernéticas (CERT, 2014).

Ciberdefensa: Capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional.

Ciberdelincuencia: Acciones ilícitas que son cometidas mediante la utilización de un bien o servicio informático.

Ciberdelito / Delito Cibernético: Actividad delictiva o abusiva relacionada con los ordenadores y las redes de comunicaciones, bien porque se utilice el ordenador como herramienta del delito, bien porque sea el sistema informático (o sus datos) el objetivo del delito.

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios (Resolución CRC 2258 de 2009).

Cibernética: Ciencia o disciplina que estudia los mecanismos automáticos de comunicación y de control o técnica de funcionamiento de las conexiones de los seres vivos y de las máquinas (RAE, 2014).

Cibernético: Adjetivo masculino y femenino para denominar todo cuanto tiene relación con la cibernética: órgano cibernético, proceso cibernético o que está especializado en cibernética, así como también a la persona que se dedica a ella (RAE, 2014).

CIBERSEGURIDAD: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

Ciberterrorismo: “La convergencia del terrorismo y ciberespacio con el fin de atacar ilegalmente ordenadores, redes e información almacenada en ellos, incluye violencia contra personas o propiedades o, al menos, genera el miedo. Abarca asesinatos, explosiones, contaminación de aguas o grandes pérdidas económicas, entre otras acciones (Dorothy Denningal, profesora de la Universidad de Georgetown)” (CONPES, 2011).

Convergencia: Evolución coordinada de redes que antes eran independientes hacia una uniformidad que permita el soporte común de servicios y aplicaciones. (Rec. UIT-T Q.1761, 3.1)

CSIRT: (Computer Security Incident Response Team) Equipo de Respuesta a Incidentes de Seguridad cibernética, por su sigla en inglés. (FIRST, 2014)

DDoS: De las siglas en inglés Distributed Denial of Service. Ataques Distribuidos de Denegación de Servicio. (http://www.rediris.es)

DOS (Denial of Service): Denegación de servicio. Servicio no disponible a una persona o proceso (aplicación) cuando es necesario (disponibilidad). (http://www.rediris.es)

Incidente Informático: Cualquier evento adverso real o sospechado en relación con la seguridad de sistemas de computación o redes de computación (http://www.cert.org/csirts/csirt_faq.html CERT/CC).

Infraestructura crítica: Es el conjunto de computadores, sistemas computacionales, redes de telecomunicaciones, datos e información, cuya destrucción o interferencia puede debilitar o impactar en la seguridad de la economía, salud pública, o la combinación de ellas, en una nación. (Resolución CRC 2258 de 2009)

IP (Internet Protocol): Etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP. (http://www.iso.org)

ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares. (http://www.iso.org)

ISO 27001: Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. (http://www.iso.org)

ISO 27002: Código de buenas prácticas en gestión de la seguridad de la información (transcripción de ISO 17799). No es certificable. (http://www.iso.org)

ISP: Proveedores de servicios de internet. En Colombia estos entes brindan adicionalmente servicios de telefonía y televisión, convirtiéndose de esta manera en unos prestadores de servicios integrales de telecomunicaciones.

Logs: Registro oficial de eventos durante un rango de tiempo en particular. Para los profesionales en seguridad informática es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué un evento ocurre para un dispositivo en particular o aplicación.

NAP (Network Access Point): Punto de conexión nacional de las redes de las empresas que proveen el servicio de acceso de Internet en Colombia, con el cual se logra que el tráfico de Internet que tiene origen y destino en nuestro país, utilice solamente canales locales o nacionales. (www.nap.com.pe)

NTC5411- 1 Gestión de la seguridad de la tecnología de la información y las comunicaciones. (Catálogo publicaciones ICONTEC Internacional)

Riesgo Informático: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. (ISO Guía 73:2002)

Seguridad Lógica: Consiste en la aplicación de barreras que resguarden el acceso a los datos y sólo se permite acceder a ellos a las personas autorizadas. (http://www.segu-info.com)

Servicios Electrónicos: e-Services, se refiere a la mejora en la facilitación de los servicios públicos a los ciudadanos a través del ciberespacio. (United Nations Educational, Scientific and Cultural Organization UNESCO)

Telecomunicaciones: Toda transmisión y recepción de signos, señales, escritos, imágenes y sonidos, datos o información de cualquier naturaleza por hilo, radiofrecuencia, medios ópticos u otros sistemas electromagnéticos.

TI: Tecnologías de la información.

TIC (Tecnologías de la Información y las Comunicaciones): Conjunto de recursos, herramientas, equipos, programas informáticos aplicaciones, redes y medios; que permiten la compilación, procesamiento, almacenamiento, transmisión de información como voz, datos, texto, video e imágenes.

Zombies: Nombre que se da a los ordenadores que han sido infectados de manera remota por un usuario malicioso con algún tipo de software que, al infiltrarse dentro del propio ordenador manipulado y sin consentimiento del propio usuario, un tercero puede hacer uso del mismo ejecutando actividades ilícitas a través de la Red. (Instituto Nacional de Tecnologías de la Comunicación España - INTECO – CERT).

Listado de Normas

A continuación se presenta un listado de Normas, relativas al tema extraído de Kosutic, D. (2012

NORMA QUE GARANTIZA LA LIBERTAD DE INFORMACIÓN

1. Ley No. 26301 Acción Constitucional de Habeas Dana, 1994.

NORMAS DE PROTECCIÓN AL DERECHO DE AUTOR

1. Decreto Legislativo No. 822 Ley sobre el Derecho de Autor (Protección Jurídica del Software), 1996.
2. Decisión No. 351 Régimen Común sobre Derecho de Autor y Derechos Conexos, 1993.
3. Resolución No. 0121-1998/ODA-INDECOPI aprueban lineamientos de la Oficina de Derechos de Autor sobre uso legal de los programas de ordenador (software), 1998.

NORMAS SOBRE DELITOS INFORMÁTICOS

1. Código Penal, 1991.
2. Ley No. 27309 Ley que incorpora los Delitos Informáticos al Código Penal, 2000.

NORMAS DE FIRMA Y CERTIFICADOS DIGITALES

1. Ley No. 27269 Ley de Firmas y Certificados Digitales, 2001.
2. Resolución Suprema No. 098-2000-JUS designan Comisión Multisectorial encargada de elaborar el reglamento de la ley de firmas y certificados digitales, 2002.
3. Resolución Ministerial No. 074-2000-ITINCI-DM designan representante del Ministerio ante la comisión multisectorial encargada de elaborar el reglamento de la ley de firmas y certificados digitales, 2000.
4. Resolución Ministerial No. 276-2000-MTC-15.01 designan representante del Ministerio ante comisión encargada de elaborar el reglamento de la ley de firmas y certificados digitales, 2001.
5. Resolución Jefatural Nº 021-2001-INEI designan representantes del INEI ante el Consejo de Supervisión e Fedatarios Juramentados con Especialización en Informática, 2001.
6. Ley No. 27310 Ley que Modifica el Artículo 11º de la Ley 27269, 2000.

NORMAS QUE PERMITEN LA UTILIZACIÓN DE LOS MEDIOS ELECTRÓNICOS PARA LA COMUNICACIÓN PARA LA MANIFESTACIÓN DE VOLUNTAD

1. Ley No 27291 Ley que modifica el Código Civil permitiendo la utilización de los medios electrónicos para la comunicación de la manifestación de voluntad y la utilización de la firma electrónica, 2000.

NORMAS QUE REGULAN EL USO DE LAS TECNOLOGÍAS DE INFORMACIÓN EN LA GESTIÓN DE ARCHIVOS Y DOCUMENTOS

1. Decreto Legislativo No. 681 Normas que Regulan el Uso de Tecnologías Avanzadas en Materia de Archivo de Documentos e Información tanto respecto a la Elaborada en Forma Convencional cuanto la Producida por Procedimientos Informáticos en Computadoras, 1991.
2. Decreto Supremo No. 009-92-JUS Aprueban El Reglamento del Decreto Legislativo No. 681, Sobre el Uso de Tecnologías de Avanzada en Materia de Archivos de las Empresas
3. Decreto Ley No. 25661 Comprenden a la Banca Estatal de Fomento, dentro de los alcances del Decreto Legislativo No. 681, en cuanto al uso de las tecnologías de microformas, microduplicados, micrograbación y otros análogos, 2008.
4. Circular No. B-1922-92-SBS Circular referida a la sustitución de archivos, mediante microformas y plazos de conservación de libros y demás documentos, 1992.
5. Resolución No. 090-93-EF-94.10.0-CONASEV Dictan normas que permitan poner en práctica el uso de tecnologías avanzadas en materia de archivo de documentos, 1993.
6. Ley No. 26612 Ley que modifica el D. LEG. No. 681, mediante el cual se regula el Uso de Tecnologías Avanzadas en Materia de Archivo de Documentos e Información, 1996.
7. Decreto Legislativo No. 827 Amplían los Alcances del D. Leg. No. 681 a las Entidades Públicas a fin de modernizar el Sistema de Archivos Oficiales, 2011.
8. Decreto Supremo No. 002-98-ITINCI Aprueban Requisitos y Procedimiento para Otorgamiento de Certificado de Idoneidad Técnica para la Confección de Microformas, 1998.
9. Decreto Supremo No. 001-2000-JUS Aprueban el Reglamento Sobre la Aplicación de Normas que Regulan el Uso de Tecnologías Avanzadas en Materia de Archivo de Documentos e Información a Entidades Públicas y Privadas, 2000.
10. Resolución Ministerial No. 169-2000-JUS Aprueban Reglamento para supervisión de eventos de capacitación, conducentes al otorgamiento de certificado de idoneidad técnica de fedatario juramentado con especialidad en informática, 2000.
11. Ley No. 27323 Ley que modifica el Decreto Ley No. 26126, 2000.

NORMAS QUE FOMENTA EL USO DE FORMATOS ELECTRÓNICOS EN LAS ENTIDADES DE LA ADMINISTRACIÓN PÚBLICA

1. Decreto Legislativo No 809 Ley General de Aduanas, 1996.
2. Decreto Supremo N° 121-96-EF Reglamento de la Ley General de Aduanas, 1997.
3. Resolución de Intendencia Nacional de Aduanas No 000 Adt/2000-000750 – Aprueban Formatos e Instructivos de la Declaración Unica de Aduanas (DUA) y la Orden de Embarque, 2000.
4. Resolución de Intendencia Nacional No 000 Adt-2000-001272 - Prorrogan entrada en vigencia de Resolución que aprueba Formatos e Instructivos de la Declaración Unica de Aduanas (DUA) y la Orden de Embarque, 2000.
5. Resolución de Intendencia Nacional de Sistemas No 001-2000- Aduanas - Estructura de Datos de la "Declaración Unica de Aduanas - Electrónica" (E-Dua), La "Orden de Embarque" y demás documentos del Despacho Aduanero Electrónico, 2000.
6. Resolución de Intendencia Nacional No 000 ADT-2000-002180 - Aprueban los Instructivos de Trabajo Declaración Unica de Aduanas (DUA) y Orden de Embarque (O/E), 2000.
7. Resolución de Intendencia Nacional de Aduanas Nş 000 ADT-2000-002797 - Modifican el Instructivo de Trabajo “Declaración Unica de Aduanas (DUA) INTA-T.00.04”, 2000.
8. Resolución de Superintendencia de Aduanas No 000103 – Establecen a nivel nacional uso obligatorio del “Formato Electrónico de Documentos Internos” (FEDI) en la tramitación interna de documentos que no estén relacionados con el despacho de mercancías, 2001.
9. Formulación y Tramitación de Documentos Institucionales – ADUANAS, 2001.
10. Resolución de Intendencia Nacional Nş 000 Adt/2001-000277 Aprueban Estructura de Solicitudes Electrónicas y Modifican El Procedimiento “Autorización de Operadores” INTA- E.00.08, 2001.
11. Resolución de Superintendencia No 002-2000/SUNAT – Dictan disposiciones referidas a La utilización de Programas de Declaración Telemática para la presentación de Declaraciones Tributarias, 2000.
12. Resolución de Superintendencia N° 044-2000/ SUNAT - Establecen disposiciones sobre Declaración y Pago de Diversas Obligaciones Tributarias, mediante Programas de Declaración Telemática, 2000.
13. Resolución del Superintendente Nacional de los Registros Públicos No 124-97-SUNARP, Aprobar la sustitución del archivo Registral existente en la Oficina de Lima y Callao por un Sistema de Microarchivos
14. Ley No 27419 Ley Sobre Notificación por Correo Electrónico, 2001.
15. Decreto Supremo No 012-2001-PCM Texto Unico Ordenado de la Ley de Contrataciones y Adquisiciones del Estado, 2001.
16. Decreto Supremo No 013-2001-PCM - Reglamento de la Ley de Contrataciones y Adquisiciones del Estado, 2001.

Referencias:

CERT. (2014). Computer Emergency Response Team. *Carnegie-Mellon University, Software Engineering Institute*. Recuperado de http://www.cert.org/csirts/csirt_faq.html CERT/CC

Center for Strategic and International Studies (CSIS). Recuperado de https://www.csis.org

Ciberseguridad (2012). Información sobre los antecedentes de la CMT. *International Telecommunications Union*. Recuperado de http://www.itu.int/en/wcit-12/documents/wcit-background-brief6S.pdf

CONPES. (2011). *Lineamientos de política para ciberseguridad y ciberdefensa (Documento CONPES 3701*). Bogotá D.C.: Consejo Nacional de Política Económica y Social, República de Colombia, Departamento Nacional de Planeación. Recuperado de http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

FireEye. (2014). FireEye, Inc. Recuperado de https://www.fireeye.com/

FIRST. (2014). FIRST.org, Inc. Recuperado de http:// www.first.org

High Representative for the European Union for Foreign Affairs and Security Policy. (02/07/2013). *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Bruselas: Comisión Europea.

Kosutic, D. (2012). *Ciberseguridad en nueves pasos: El Manual sobre seguridad de la información para el Gerente*. Zagreb: Advisera Expert Solutions Ltd. Recuperado de http://www.iso27001standard.com

Presidencia del Gobierno, Departamento de Seguridad Nacional. (2013). *Estrategia de Seguridad Nacional*. Madrid: Gobierno de España. Recuperado de www.dsn.gob.es/es/file/146/download?token=Kl839vHG

RAE. (2014). Real Academia Española. Recuperado de www.rae.es

Sutherland, B. (2011). *The Economist: Modern Warfare, Intelligence and Deterrence. The technologies that are transforming them*. London: Profile Books.