COLEGIO DE DEFENSA NACIONAL

ORDINARIO

Ejemplar No._____

LA SEGURIDAD NACIONAL ANTE LOS RETOS DE LAS NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN

(COMPILACIÓN)

Mayo de 2011

INDICE

Introducción

El pueblo cubano siempre ha estado sometido a numerosas amenazas y agresiones de todo tipo, tanto de orden natural, como los huracanes y sismos que con cierta frecuencia nos afectan, hasta la proveniente de potencias extranjeras interesadas en explotar los recursos económicos del país.

Con el triunfo de la Revolución, estas amenazas y agresiones se multiplicaron. Tan sólo dieciséis días después del triunfo, el líder de la Revolución, compañero Fidel Castro denunciaba: "*…la campaña ha sido de grandes proporciones y tiene que obedecer a determinados intereses. Partió, en primer lugar, de las agencias de cables internacionales, y yo puedo dar cuenta de la mala fe con que han procedido las agencias de cables internacionales (…) han atacado, han calumniado y han llevado adelante su campaña miserable y cobarde (…) Pero ¿qué se pretende? Antes que nada: restarnos la opinión pública internacional, aislarnos*"[1]. Puede asegurarse entonces que la primera agresión sufrida por la naciente Revolución, de parte del imperio, se desarrolló, precisamente, en la esfera de la **información.**

Las tecnologías de la información, entendidas como aquellas que permiten el procesamiento, conservación y diseminación de la información en la sociedad, sufrieron un cambio trascendental a partir del desarrollo de la tecnología digital y de las redes de datos en la segunda mitad del pasado siglo, especialmente con la explosión de desarrollos tecnológicos, como Internet, y la masificación de estas tecnologías que ha tenido lugar en los últimos 20 años.

Como toda revolución tecnológica, esta trajo innumerables ventajas y oportunidades para la sociedad, a las cuales no sólo no podemos renunciar, sino que tenemos que expandir y aprovechar al máximo, en interés del desarrollo económico y social de nuestra nación; pero paralelamente, introdujo también nuevos peligros y retos que tenemos que enfrentar con inteligencia, racionalidad y decisión.

La aparición de diversos fenómenos negativos asociados al uso de estas nuevas tecnologías en el país, el análisis de las tendencias crecientes que se aprecian en algunos de ellos, y la valoración de los escenarios futuros que podemos prever en este campo, llevaron a la dirección del país a organizar cursos para los principales cuadros que responden por la informatización y la seguridad de la información en las diferentes instancias del país.

El presente material, se elaboró como bibliografía de consulta principal para estos cursos, compilando un conjunto de textos elaborados como base de las conferencias a impartir, así como de otros materiales de interés relacionados con el tema, que los alumnos podrán estudiar de forma independiente.

Los autores que intervinieron en su confección fueron: Cor Lidia María Garrigó Andreu, DrC Profesora Titular del Coden ("*Fundamentos de la Seguridad Nacional de Cuba"*); TCor Juan Carlos Garnier Galán, DrC Profesor Titular del Coden ("*Fundamentos de la Seguridad de la Información"*; "*El empleo de la desinformación a través de los medios de comunicación masiva como un problema de seguridad nacional e internacional"; "Selección de referencias sobre la importancia y el papel de la información, realizadas por el líder de la Revolución Fidel Castro Ruz"; y "Glosario sobre programas malignos y otras amenazas a la Seguridad informática*), Roberto del Puerto Alonso, Director de la Oficina para la Informatización del MIC ("*El*

[1] Castro Ruz, Fidel. "Discurso pronunciado en Pinar del Río el 17 de enero de 1959". Periódico Granma. 17 de enero de 2009. Pág. 3

desarrollo de la informática y las comunicaciones, y *la Sociedad de la Información. Oportunidades y amenazas para la Seguridad Nacional"*; así como "*La informatización de la sociedad cubana"*); Rosa Miriam Elizalde Zorrilla, Editora de Cubadebate ("*Internet y la ciberguerra"*; *"Las redes sociales. Oportunidades y amenazas para la Seguridad Nacional"; "Los 10 servicios de redes sociales más populares en el 2010"* y *"Redes sociales: Lo esencial sigue siendo tomar La Bastilla*"); Pedro Andrés Urra González, Director de Infomed ("*Apuntes sobre la red de información y comunicación del Sistema Nacional de Salud de Cuba: Infomed"*), José Alejandro Bidot Peláez, Director de Segurmática ("*Programas malignos y otras amenazas a la Seguridad informática. Acciones para su enfrentamiento"*); Gonzalo García Pierrat, Subdirector de la OSRI del MIC ("*Deficiencias más comunes de la Seguridad Informática en Cuba"*), TCor Armando Morales Castrillón, Jefe de Departamento, Minint ("*Indisciplinas principales asociadas a la seguridad y protección de la Información Oficial"*).

En la confección de este material se respetaron los estilos de redacción y contenidos expresados por los respectivos autores.

La Dirección del Colegio de Defensa Nacional agradecerá que se le hagan llegar las opiniones sobre este material de estudio, con el fin de perfeccionarlo para ediciones futuras.

I- Fundamentos de la Seguridad nacional de Cuba

El tema de la **Seguridad** es hoy centro de discusión en el mundo y un concepto aceptado por la comunidad internacional. En su utilización generalmente se relacionan tres elementos: el bien a preservar, los medios a utilizar y la definición de las amenazas y, por consiguiente, del "enemigo"; tiene un contenido clasista, vinculado al surgimiento del Estado cuya proyección de seguridad se ha basado en el cumplimiento de los intereses de la clase dominante. Por tanto, seguridad nacional es un concepto de naturaleza política pues busca asegurar la supervivencia de la nación, que es el bien más preciado.

"Vivimos en un mundo interesante, excepcional, […] un mundo en plena fase de globalización que trae problemas tremendos y desafíos inmensos […]", afirmó el Comandante en Jefe, *"[…] nuestro mayor interés es que nuestro pueblo, en sus conocimientos, en su cultura y, sobre todo, en su conciencia política y científica, se encuentre preparado para ese mundo que se nos viene encima y que marcha a pasos de gigantes".*[2]

Teniendo en cuenta lo anterior y que las relaciones internacionales han venido sufriendo constantes e importantes cambios, resulta conveniente dar tratamiento y utilización al término de seguridad nacional, acorde con las realidades y circunstancias que impone el mundo globalizado de hoy.

La seguridad nacional de cada Estado es indivisible de la seguridad internacional, lo que implica que debe conjugarse con la de los otros, sobre la base del respeto a los principios de la **Carta de las Naciones Unidas**. Tanto la seguridad nacional como la internacional deben ser consideradas como cuestiones de **grado;** cada vez es más frecuente la necesidad de enfrentar amenazas que se salen fuera del control directo de una nación. Se trata entonces de un estado cuya plenitud resulta difícil de lograr.

Indudablemente, la realidad cubana tiene un impacto en ese mundo. Cuba es un pequeño país estable políticamente, con conciencia política, con resultados palpables en todas las esferas, con garantías sociales para sus ciudadanos, con un sistema social justo y equitativo, libre en su acción internacional, solidario, internacionalista, que se esfuerza por elevar la cultura general integral como expresión de soberanía y libertad, que se mantiene por la fuerza de sus ideas y la convicción martiana de que *"perdura, lo que un pueblo quiere".*[3]

En la política cubana queda demostrado claramente el carácter defensivo de su concepción militar y la lucha permanente y sistemática contra azotes internacionales de esta época que afectan la seguridad nacional de los Estados. Cuba hará cumplir las leyes que soberanamente se ha dado y ha expresado su disposición a cooperar con todos los países con pleno respeto por el derecho internacional, conscientes de que las relaciones con cualquier otro Estado no serán jamás negociadas bajo agresión, amenaza o coerción de una potencia extranjera[4].

Constituye por tanto una necesidad fundamentar teóricamente la concepción de Seguridad Nacional de Cuba, basada en su historia y práctica revolucionaria ante la agresividad de su principal enemigo, empleando códigos y terminologías reconocidas internacionalmente. Esto es útil para ofrecer un nuevo enfoque de seguridad nacional como variante opuesta y alternativa al

[2] Castro Ruz Fidel. Discurso pronunciado en Santiago de Cuba, en ocasión del 45 Aniversario del Asalto al Cuartel Moncada, julio 26 de 1998.
[3] Martí Pérez José. "El Partido Revolucionario Cubano". Patria, 3 de marzo de 1892.
[4] Constitución de la República de Cuba. Artículo 11. La Habana, 2005.

enfoque de seguridad nacional visto desde el Primer Mundo y especialmente desde Estados Unidos, que le pueda servir a los países del Sur y a todos aquellos que pretendan mantener su soberanía y no ser aplastados por el imperialismo neoliberal.

Cuba, a partir del diferendo histórico con los Estados Unidos, caracterizado por las posiciones de intereses geopolíticos y la propia política guerrerista, hegemónica y hostil de este país, ha sufrido y encara aún agresiones y amenazas de todo tipo que afectan nuestros intereses nacionales, lo que implica la necesidad de formular y definir con gran claridad los fundamentos de la seguridad nacional.

1.1 Conceptos básicos de la Seguridad nacional de Cuba.

Para Cuba el concepto de seguridad nacional, no incluye la defensa de objetivos hegemónicos, expansionistas ni extraterritoriales que sobrepasen sus fronteras naturales y afecten la seguridad nacional de otros países, y mucho menos de los EUA, salvo la que emane de su ejemplo en la aplicación de un sistema más justo y participativo.

El contenido del concepto de Seguridad Nacional de Cuba está indisolublemente relacionado a su lucha por la independencia y soberanía nacional. El origen o los antecedentes de las intenciones norteamericanas sobre Cuba están presentes desde la etapa del nacimiento de la nación norteamericana que es anterior al surgimiento de la nación cubana. Estas intenciones, desde entonces, estaban asociadas a impedirnos llegar a ser una nación. La pretensión de dominar a Cuba se convirtió en doctrina y práctica de las diferentes administraciones norteamericanas.

En el caso de Cuba la seguridad nacional refleja la defensa de los intereses de la mayoría, por eso se identifica con **la seguridad del pueblo,** y su base filosófica se sustenta en dos pilares fundamentales: el marxismo-leninismo y el pensamiento estratégico de la Revolución Cubana cuyos máximos exponentes son José Martí y el compañero Fidel.

La Seguridad Nacional de Cuba, tiene su fundamento en la Constitución de la República, los principios éticos que sustentaron el origen de la nación, el respeto al Derecho Internacional y los principios de la Carta de las Naciones Unidas y es garantizada por el Estado, con la participación activa del pueblo bajo la dirección del Partido Comunista de Cuba, a través del ejercicio de las funciones y atribuciones que les confiere la ley y otras disposiciones legales.

El concepto de **Seguridad Nacional de Cuba** se define como: ***la condición necesaria alcanzada por el país, en correspondencia con su poderío nacional, que le permite prever y acometer acciones, para el logro y la preservación de sus intereses y objetivos nacionales, pese a los riesgos, amenazas y agresiones de carácter interno y externo.***

Esta condición (estado) necesaria alcanzada por el país, es el resultado de las acciones que se realizan en el proceso de construcción y defensa de la sociedad socialista, en dos grandes direcciones: en interés del **desarrollo sostenible** y **la defensa de la Revolución Cubana** ante cada tipo de riesgo, amenaza o agresión.

Los intereses nacionales están vinculados a la supervivencia misma de la nación, por lo que tienen un carácter vital, cuya preservación es un reto en este mundo unipolar, globalizado y específicamente en medio del conflicto EE.UU.-Cuba. Su definición es: todos aquellos valores y aspiraciones en las diferentes esferas del país, de importancia prioritaria para la nación, con un largo plazo de permanencia y que determinan y se expresan en los objetivos nacionales y en las estrategias para alcanzarlos.

La dinámica de los intereses en general viene dada porque ningún interés particular o especial puede estar nunca por encima de los intereses de la nación; también está muy presente la relación que estableció José Martí cuando expresó: *"Patria es humanidad"*.[5]

Los **objetivos nacionales** constituyen metas a alcanzar en determinada fase de la evolución histórico-cultural de la nación y trazan las principales direcciones para alcanzar los intereses nacionales. Representan el punto referencial fundamental para la planificación estratégica del país y guían la vida de la sociedad.

Los objetivos nacionales están enunciados esencialmente en la Constitución de la República y están dirigidos a: mantener los fundamentos políticos, sociales y económicos establecidos en la Constitución de la República; encauzar los esfuerzos de la nación en la construcción del socialismo; mantener y fortalecer la independencia, soberanía, integridad territorial, unidad, identidad cultural y autodeterminación de la nación cubana; garantizar la libertad y la dignidad plena del hombre; lograr el desarrollo sostenible; impulsar la integración y colaboración con los pueblos, en particular de América Latina y el Caribe.

Luchar para que sea eliminado el terrorismo a escala global en cualquiera de sus manifestaciones y toda expresión de corrupción, también constituyen objetivos nacionales importantes.

En las condiciones de Cuba, resulta vital mantener la **identidad nacional** como mayor soporte político del país, definiéndose esta como: el auto reconocimiento de los rasgos más representativos de la cultura, sociedad e ideología que identifican al pueblo cubano, su idiosincrasia, y lo distinguen dentro de la comunidad de naciones, que se forjaron a lo largo del desarrollo de procesos como el surgimiento de la nación, la lucha por la independencia, la soberanía y la construcción del socialismo.

El **poderío nacional**, es la capacidad del país para poner en acción los potenciales de la nación para la consecución de los intereses y objetivos nacionales.

El Comandante en Jefe expresó:"*La fuerza de un país pequeño como Cuba, no es militar, no es económica, es moral*",[6] las propias tradiciones de lucha, las raíces históricas y étnicas que fundaron la nación y su cultura forman parte del poderío nacional el que, sin duda, tuvo sus oportunidades de desarrollo pleno a partir del triunfo de la Revolución. La unidad es la clave del poderío nacional.

Los **potenciales de la nación** constituyen las posibilidades máximas de que dispone el país en todo tipo de recursos en las esferas político-moral, económico-social, científico-tecnológico, militar, de relaciones exteriores y otros, en estado latente, los cuales pueden ser transformados en poderío nacional. En la base de los potenciales de la nación está el **capital humano,** que pertrechado con la Ideología de la Revolución Cubana sirve a su pueblo y a la humanidad.

"El secreto está" -dijo el compañero Fidel- *"en el hecho real de que el capital humano puede más que el capital financiero" y* lo define como: "***Capital humano*** *implica no solo conocimientos, sino también y muy especialmente, conciencia, ética, solidaridad, sentimientos verdaderamente humanos, espíritu de sacrificio, heroísmo y la capacidad de hacer mucho con muy poco"*.[7]

---

[5] Martí Pérez, José. "En casa", Patria, Nueva York. 26 de enero de 1895. OC t.5, p. 468.
[6] Castro Ruz, Fidel. Informe Central al II Congreso PCC, 1980.
[7] Castro Ruz, Fidel. Discurso en el acto de graduación de la ELAM. 20 de agosto del 2005.

En su discurso en la Universidad de la Habana, el Comandante en Jefe expresó: *"El capital humano no es producto no renovable; es renovable, pero además multiplicable. Cada año el capital humano crece y crece… el capital humano es, o avanza aceleradamente para ser el más importante recurso del país, muy por encima de casi todos los demás juntos […] vale mucho más que el petróleo".*[8]

Todos estos potenciales se integran y desarrollan su actividad sobre la base de los **principios de la democracia socialista.** En lo interno la seguridad nacional también radica en una combinación armónica de un sistema político que garantiza una amplia democracia participativa, con un sistema económico y social que busca la más plena justicia y equidad, junto al compromiso de los dirigentes con el pueblo que los ha elegido.

Con el empleo de todos los potenciales de la nación, mediante la aplicación consecuente del desarrollo sostenible y la defensa de la Revolución Cubana ante cada tipo de riesgo, amenaza y agresión se garantiza la Seguridad Nacional de Cuba. Estos pilares están íntimamente relacionados, cada uno por si solo no garantiza la seguridad nacional, ya que ambos convergen hacia un mismo fin, alcanzar los intereses y objetivos nacionales. Esto requiere de un equilibrio entre objetivos, las vulnerabilidades que es preciso eliminar o atenuar, los recursos y las posibilidades existentes.

El Artículo 8 de la Ley No. 81 del Medio Ambiente de la República de Cuba define el **desarrollo sostenible** como: "El proceso de elevación sostenida y equitativa de la calidad de vida de las personas, mediante el cual se procura el crecimiento económico y el mejoramiento social, en una combinación armónica con la protección del medio ambiente, de modo que se satisfagan las necesidades de las actuales generaciones, sin poner en riesgo las de futuras generaciones".[9]

La cultura resulta el medidor por excelencia de la calidad del desarrollo. A su vez la justicia es una categoría de la cultura, que concibe el pleno desarrollo del ser humano.

A pesar de todos los esfuerzos que ha hecho el enemigo para dividirnos, para destruir la Revolución, el pueblo está organizado, preparado e integrado con todos los elementos que conforman la sociedad dirigida por el Partido Comunista y que dan como resultado la unidad. El pueblo ha demostrado **capacidad y voluntad de resistencia y de lucha**, tiene una cultura política sólida, convicciones y valores importantes que defender.

La defensa de la Revolución Cubana es el conjunto de acciones coordinadas que la nación opone, en todo momento, a cada tipo de riesgo, amenaza o agresión con el fin de preservar sus intereses y objetivos nacionales y mantener el orden constitucional**.** Es la respuesta de la sociedad agredida y amenazada en cualquiera de sus esferas de actuación: económica, política, social, militar, ideológica, cultural, medioambiental y otras. Es la categoría más abarcadora en lo que a defensa se refiere.

Para enfrentar una agresión militar externa, se prepara desde tiempo de paz la **Defensa Nacional**, que es parte componente de la defensa de la Revolución Cubana.

La seguridad nacional no es estática, evoluciona, porque continuamente el país se encuentra sometido a nuevos riesgos, amenazas y agresiones, lo que exige que esta se adecue en correspondencia con las circunstancias imperantes.

[8] Castro Ruz, Fidel. Discurso en la Universidad de La Habana. 17 de noviembre del 2005.
[9] Ley No. 81 del Medio Ambiente de la República de Cuba. 11 de junio de 1997.

Cada día se libran importantes batallas para hacer avanzar la Revolución, contra todo lo que pretenda frenarla, hacerla retroceder o destruirla. Fortalecer y preservar la Revolución es el principal objetivo y desafío que tiene la Seguridad Nacional de Cuba.

La Seguridad Nacional de Cuba se sustenta en los siguientes **principios generales:**

a) El fortalecimiento de la unidad del pueblo en torno al Partido Comunista de Cuba, su vanguardia revolucionaria.

b) El perfeccionamiento constante del carácter participativo del sistema político cubano, socialista y genuinamente democrático, y de su legalidad e institucionalidad.

c) La utilización óptima y la constante valorización del capital humano del país, como factor determinante en la construcción del socialismo en Cuba.

d) La consolidación de la propiedad socialista como factor organizador de la producción, distribución y redistribución del producto social de Cuba.

e) Basarnos en los esfuerzos propios y sistemáticos para preservar y ampliar la obra de la Revolución Cubana.

f) La continua aplicación de un enfoque de sostenibilidad al desarrollo integral del país, así como de mitigación y adaptabilidad ante el deterioro medioambiental a nivel global.

g) No descuidar jamás la preparación del país para la defensa bajo la concepción estratégica defensiva de Guerra de Todo el Pueblo.

h) La permanente vigilancia revolucionaria y el enfrentamiento tanto a las acciones del enemigo dirigidas a subvertir el orden político, económico y social establecido, como a los delitos y conductas antisociales que pueden afectar la estabilidad interna del país.

i) La marcada vocación antiimperialista, solidaria, de cooperación e integracionista, que garantice un amplio y variado nivel de relaciones del país con la comunidad internacional.

j) La protección oportuna e integral de la población, la infraestructura social y la economía del país, y su recuperación en base a prioridades ante situaciones de desastres y excepcionales.

El enfoque cubano de seguridad nacional es amplio, multidimensional.

La seguridad nacional comprende diferentes **dimensiones,** que son las distintas esferas del país, que por su sensibilidad económica, política, social y militar, son de vital importancia para el sostenimiento de la misma. Estas se clasifican de acuerdo al tipo de actividad en: la seguridad político-moral, la seguridad económico-social, la seguridad militar, la seguridad interior, la seguridad exterior, la seguridad jurídica, la seguridad científico-tecnológica, la seguridad ambiental, la seguridad ante desastres, y la seguridad de la información, que será la que nos ocupe especialmente en este texto. Todas ellas tienen un componente material y otro espiritual.

La siguiente frase expresada por el Comandante en Jefe en alusión a Martí, sintetiza la esencia del **concepto de Seguridad Nacional de Cuba:** *"El mayor monumento de los cubanos a su memoria es haber sabido construir y defender esta trinchera, para que nadie pudiera caer con una fuerza más sobre los pueblos de América y del mundo".*[10]

[10] Castro Ruz, Fidel. Discurso. Conferencia Internacional "Por el Equilibrio del Mundo". Periódico Granma, 30.01.2003.

1.2- Principales riesgos, amenazas, agresiones y desafíos que enfrenta la Seguridad nacional.

Se debe entender por **riesgo,** la posibilidad y proximidad de que suceda un daño; por **amenaza**, la percepción, insinuación o afirmación de que se va a hacer un daño (es sinónimo de peligro); constituye todo aquello que directa o indirectamente, puede poner en peligro a una nación, a sus ciudadanos o a sus intereses, y por **agresión**, la acción hostil que causa un daño.

Estos términos están asociados con la **vulnerabilidad:** atributo de la nación o de sus potenciales que indica que se puede ser afectado de manera tal, ante una acción de cualquier tipo, que implique una disminución sensible de las posibilidades de cumplir los intereses y objetivos nacionales y por tanto sufrir un daño de consideración. El riesgo es función de la amenaza y la vulnerabilidad; de ahí que el riesgo sea directamente proporcional a la vulnerabilidad e inversamente proporcional a la **invulnerabilidad**. La invulnerabilidad es un atributo de la nación o sus potenciales, que indica que la acción que pueda recibir no impide cumplir, en la esfera de que se trate, los intereses y objetivos nacionales; está asociada a un elevado grado de irreversibilidad del proceso revolucionario en la esfera dada y expresa un alto nivel de seguridad nacional.

Los principales riesgos, amenazas y agresiones a la Seguridad Nacional de Cuba, se derivan de la agresiva y hostil política de los círculos de poder imperialistas, que desde el propio triunfo de la Revolución, han promovido su destrucción por todas las vías posibles, que van desde la agresión política, militar, económica, biológica, psicológica, ideológica, radial y televisiva, cultural, diplomática e informática, hasta acciones de carácter terrorista, planes de eliminación física de los principales dirigentes, estimulación de la subversión interna, campañas de descrédito y otras que son suficientemente conocidas por el pueblo y denunciadas reiteradamente ante los organismos internacionales.

El bloqueo económico, comercial y financiero impuesto por los EUA a Cuba[11] y rechazado por la comunidad internacional, califica como un verdadero acto de genocidio, al tratar de rendir por hambre y enfermedad a un pueblo decidido a continuar siendo libre e independiente.

En el complejo escenario internacional, caracterizado por la hegemónica actuación unilateral de los Estados Unidos, con absoluto desconocimiento de las leyes y organismos internacionales, unido a la adopción de nuevas concepciones de seguridad y defensa, que incluyen las llamadas "acciones preventivas", bajo la justificación del enfrentamiento al "terrorismo" y la inclusión de Cuba en su lista de países patrocinadores, se incrementan los riesgos y amenazas de una agresión militar directa contra el país, que intentarían legitimar bajo diferentes pretextos.

Se integran a estos riesgos y amenazas, la acción de los grupos terroristas y mafiosos anticubanos y la influencia que estos ejercen en el gobierno norteamericano, la manipulación del conflicto y del potencial migratorio hacia los Estados Unidos (que promueve la asesina Ley de Ajuste Cubano), el accionar de sus servicios especiales y en particular las provocaciones desde la Oficina de Intereses de EE.UU. en La Habana.

Todo ello con el objetivo de promover la contrarrevolución interna, el surgimiento de incidentes y desórdenes internos, las pretensiones de vincular a Cuba con el narcotráfico internacional, el

[11] El bloqueo fue establecido oficialmente bajo la administración del presidente J. F. Kennedy, cuando el 3 de febrero de 1962, firmó la orden ejecutiva presidencial 3447; y el 6 del mismo mes, la Resolución Federal no. 1085, que entró en vigor al día siguiente.

tráfico humano y la tergiversación de la solidaria ayuda que ésta brinda a procesos democráticos en la región; todo lo cual constituyen condiciones que bajo determinadas circunstancias pueden enrarecer el clima bilateral y generar incidentes que sirvan de pretextos para desencadenar escaladas agresivas, sin descartar la ejecución de la agresión militar.

Aumenta la guerra psicológica por parte del enemigo, que concentra sus medios de propaganda contra Cuba, con decenas de miles de horas mensuales de transmisión radial y televisiva a través de numerosas emisoras enemigas, de carácter subversivo, que violan nuestro espectro radioeléctrico.

El archipiélago cubano es altamente vulnerable al cambio climático global, dada su condición de pequeño estado insular situado en la región tropical del planeta. Los riesgos están directamente asociados al incremento paulatino de la temperatura y el nivel medio del mar, los regímenes cambiantes en las precipitaciones y el aumento de la intensidad de eventos meteorológicos extremos.

En lo interno, surgieron en los años de Período Especial, un conjunto de fenómenos totalmente ajenos a los principios de la Revolución Cubana, que constituyen nuevos riesgos y amenazas para la seguridad nacional, entre los que resaltan: la corrupción, las indisciplinas sociales, la recepción ilegal de señales de radio y televisión subversivas y el empleo de los medios automatizados personales y del estado con estos fines, las marcadas desigualdades, la delincuencia, el tráfico y el consumo de drogas. Tales fenómenos no pueden dejar de considerarse, por el juego que le hacen a las intenciones y planes del enemigo, por lo que exigen y exigirán de enérgicas medidas de respuesta.

El Comandante en Jefe en su discurso en la Universidad de La Habana, el 17 de noviembre del 2005, reflexionó profundamente ante los errores cometidos, las desigualdades, el robo, el desvío de recursos, la corrupción que existen en el país y el peligro que corre la Revolución de que la destruyamos nosotros mismos, aunque no podría ser destruida por el enemigo, el gobierno norteamericano.

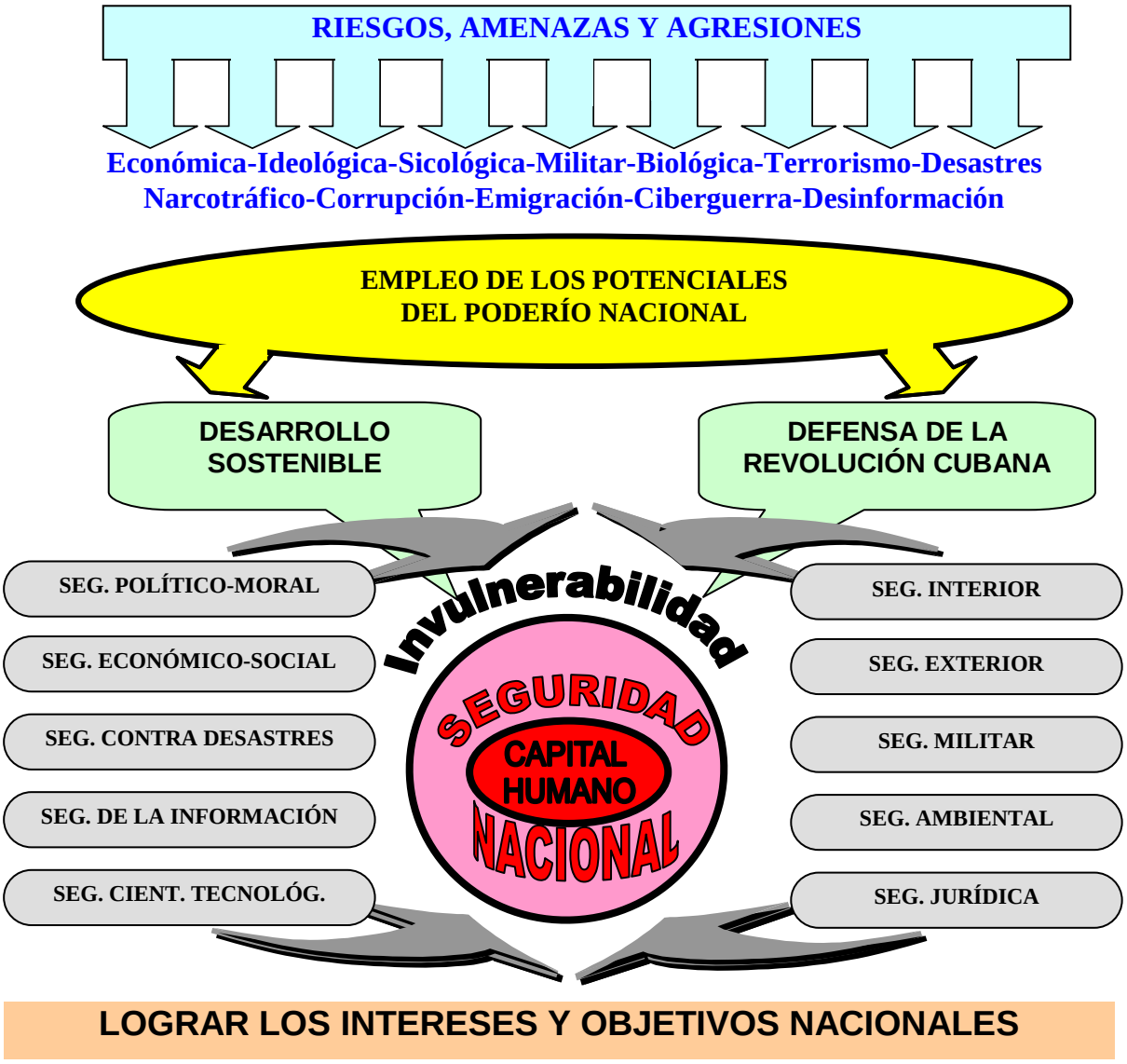
En medio de los riesgos y amenazas señalados, los principales desafíos que enfrenta actualmente la Seguridad Nacional de Cuba para el logro de sus intereses y objetivos nacionales son:

- Avanzar en la construcción socialista en el mundo globalizado de hoy, conviviendo con determinados valores de la sociedad de consumo, sin perder los principios y por lo tanto la esencia social de la Revolución.
- Impulsar el desarrollo económico y social sobre bases sostenibles
- Lograr efectividad en la gestión económica en condiciones de bloqueo, sin renunciar al objetivo políticamente estratégico de crear una conciencia comunista.
- Garantizar la preparación del país para la defensa ante una agresión militar por parte de un enemigo que cuenta con un superior poderío económico, tecnológico y militar.
- Garantizar la preparación del país en las medidas relacionadas con la reducción de los desastres (de origen natural, tecnológico o sanitario).[12]
- Continuar la lucha decisiva en el campo diplomático por el rompimiento del aislamiento que se le pretende imponer a la Revolución Cubana y la eliminación del bloqueo.

[12] Directiva No. 1 del Presidente del Consejo de Defensa Nacional para la planificación, organización y preparación del país para situaciones de desastres. 8 de abril de 2010.

- Luchar por la integración latinoamericana y caribeña, y la globalización de la solidaridad.
- Enfrentar la fuerte agresión radial y televisiva contra Cuba y elevar la preparación política e ideológica de nuestro pueblo ante las campañas mediáticas de desinformación del enemigo.
- Garantizar u uso ordenado y masivo de las tecnologías de la información como parte del proceso de informatización de la sociedad que contribuya a la soberanía e independencia tecnológicas.

En síntesis, la experiencia cubana demuestra que en última instancia, la seguridad nacional de un pequeño Estado descansa en las propias fuerzas del pueblo, que ha elegido su sistema político, económico y social, en su unidad, cultura, en el consenso para alcanzar los intereses y objetivos nacionales y en la capacidad y voluntad de resistencia para desarrollarse, defenderse y vencer en las más difíciles circunstancias**.**



II- Fundamentos de la Seguridad de la información

Probablemente ningún concepto tiene tanta trascendencia en la vida de las personas y las sociedades, y al mismo tiempo resulta tan poco consensuado como es el de **información**.

De forma general puede considerarse la información como una propiedad de la materia, resultado de su diversidad, que le permite ordenarse en el tiempo o en el espacio de modo tal que pueda ser reconocida por formas superiores de organización mediante receptores especialmente adaptados para ello, produciendo en estas, efectos específicos.

A los efectos de este material[13], asumiremos como definición particular de **Información**, el ***conjunto de datos estructurados de forma significativa, que permite a los individuos u organizaciones el conocimiento de sí mismos y del mundo en que se desenvuelven y, a partir de este, la toma de decisiones para su actuación.***

Toda la actividad humana, desde la misma aparición del hombre, constituye un proceso de constantes tomas de decisiones y de aprendizaje consciente, cuyas bases están precisamente en la disponibilidad de información. Los seres vivos, y en particular los humanos y las estructuras sociales que ellos conforman, no pueden subsistir sin información sobre el entorno natural y social en que conviven.

Por ello, para un Estado, la información constituye un **recurso estratégico**, que se consume constantemente por todas sus estructuras y componentes, desde sus ciudadanos, hasta sus más complejos sistemas de dirección; empleándose en la toma de decisiones de todo tipo: personales, económico-financieras, políticas, militares; incluyendo las más trascendentes para la vida de la nación e incluso de todo el planeta, y como tal, forma parte del Poderío Nacional.

Como cualquier otro recurso material, el valor de uso de la información varía con el tiempo, y es esencial su disponibilidad en el momento y lugar en que se necesite emplear. La información puede ser almacenada y es susceptible de robo, degradación y destrucción. Tres características fundamentales que la distinguen de otros recursos son la posibilidad de ser trasladada instantáneamente entre dos puntos distantes; la posibilidad de multiplicarla; y la posibilidad de modificar su forma sin detrimento de su contenido.

La importancia de la información ha ido aumentando con el desarrollo y complejización de las estructuras socioeconómicas, al punto, que se considera que la humanidad, luego de transitar por las llamadas eras agrícola e industrial, se halla actualmente en la era de la información.

Al respecto nuestro Comandante en Jefe expresó: "*Y un pueblo —tengan la seguridad— no solo **será más rico** mientras más fábricas posea, o más minerales, o más materias primas descubra: un pueblo será por encima de todo más rico cuanto más cultura política tenga, cuanto más preparación tenga, **cuanto más información tenga**…*"[14].

[13] La información es utilizada por los seres vivos desde sus formas más elementales, como la información genética durante la reproducción, pero este tipo de información no es la que abordaremos aquí y por tanto no resulta de interés su abordamiento teórico.

[14] Discurso pronunciado en el acto celebrado con motivo de la terminación del montaje de una unidad en Tallapiedra de la Empresa Eléctrica, el 23 de julio de 1972

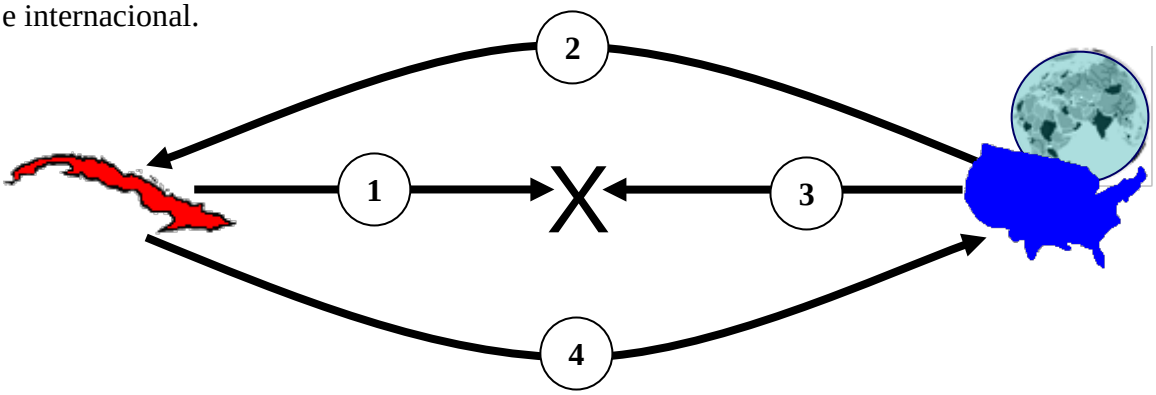
2.1 Información de interés para la seguridad nacional

La variedad y volumen de información existente es prácticamente infinita y no toda tiene una incidencia significativa en la Seguridad Nacional. Por tanto, se debe entender por **Información de interés para la Seguridad Nacional**[15] a aquella que pueda servir de algún modo:

- *al enemigo para conocer nuestras vulnerabilidades, o ayudarlo en la preparación y realización de agresiones contra el país,*
- *a los dirigentes y órganos de dirección y mando para adoptar decisiones, y cumplir las funciones a ellos asignadas,*
- *a los ciudadanos para el desarrollo de nuevos conocimientos sobre la naturaleza o la sociedad que incidan decisivamente en los planes y programas de desarrollo sostenible del país o de la defensa de la Revolución Cubana.*
- *a conformar estados de opinión sobre la Revolución Cubana dentro o fuera del país.*
- *para ejecutar, de forma automatizada, acciones no autorizadas que provoquen la sustracción, destrucción o alteración de otras informaciones; o alteren el buen funcionamiento de sistemas informáticos.*

Por sus características, origen, destino y empleo, esta información puede clasificarse, de forma general, como sigue:

1. Información oficial u otra que se origina y emplea en el país, que requiere ser protegida.
2. Información originada en el exterior, de interés para el país, que se necesita obtener.
3. Información perniciosa originada en el exterior o producida en el país, a la que se debe impedir su diseminación en el espacio informativo nacional.
4. Información sobre el país que resulta conveniente dar a conocer a la opinión pública nacional e internacional.



Se denomina **Información Oficial**, a aquella información *"que posee un órgano, organismo, entidad u otra persona natural o jurídica residente en el territorio nacional o representaciones cubanas en el exterior, capaz de proporcionar directa o indirectamente datos o conocimientos que reflejen alguna actividad del Estado o reconocida por éste, y que pueda darse a conocer de cualquier forma perceptible por la vista, el oído o el tacto. Es un bien del órgano, organismo o entidad que la posea"*[16]

A los fines de establecer las medidas para su seguridad, la información oficial se divide en tres grupos: **Clasificada; Limitada y Ordinaria**

[15] En lo adelante, al emplear el término **información**, nos refereriremos a esta información en particular.
[16] Decreto-Ley 199 del 2 de diciembre de 1999. Capítulo III, artículo 5.

Se establece que la información **Clasificada** es la que "*requiere de medidas de protección definidas por Ley, por contener datos o informaciones cuyo conocimiento o divulgación no autorizada puede ocasionar daños o entrañar riesgos para el Estado o para su desarrollo político, militar, económico, científico, cultural, social o de cualquier otro tipo*" [17], mientras que la **Limitada** es la que "*sin poder ser conceptuada como clasificada, por su importancia o carácter sensible para el objeto social del órgano, organismo, o entidad u otra persona natural o jurídica que la posee, no resulta conveniente su difusión pública y debe limitarse su acceso a personas determinadas que no podrán destruirla, divulgarla ni modificarla sin la correspondiente autorización"*[18]

A su vez la información clasificada puede tener las categorías de Confidencial, Secreto o Secreto de Estado, los cuales se establecen a partir de la "*Lista General del Estado cubano*", así como de la "*Lista interna para la clasificación y desclasificación de la Información oficial*" que elabora cada organismo o entidad.

La categoría Secreto de Estado es aquella cuyo conocimiento o divulgación no autorizada puede poner en peligro la seguridad, integridad, estabilidad o el funcionamiento del Estado; la categoría Secreto es aquella cuyo conocimiento o divulgación no autorizada puede causar perjuicios en las esferas política, militar, económica, científica, técnica, cultural, social o cualquier otra de importancia para el funcionamiento del estado; y la categoría Confidencial es aquélla cuyo conocimiento o divulgación no autorizada puede ocasionar daños a la producción, los bienes, los servicios y en general a la gestión de cualquiera de ellos[19].

Partiendo de las definiciones antes expuestas, queda claro que no toda información de interés para la seguridad nacional es información oficial, ni toda información oficial es de interés para la seguridad nacional; pero igualmente, que toda información oficial clasificada es, "*per se*", información de interés para la seguridad nacional.

2.2- Principales conceptos sobre Seguridad de la información.

La Seguridad de la Información es una de las dimensiones de la Seguridad Nacional de Cuba.

Se considera la **Seguridad de la Información** como: *la condición necesaria alcanzada por el país en la cual se garantiza la disponibilidad, confidencialidad e integridad de la información que este necesita emplear para su desarrollo y defensa; se dificulta o impide el empleo ilegal o pernicioso del espacio informativo nacional; y se garantiza la divulgación de la verdad sobre la Revolución cubana y las amenazas o agresiones a que es sometida.*

Expuesto de forma más didáctica:

[17] Ibidem. Capítulo III, artículo 7
[18] Ibidem. Capítulo III, artículo 17
[19] Ibidem. Capítulo III, artículos 9, 10 y 11

1- Se busca, obtiene, disemina y organiza la información, de forma tal que todo usuario autorizado que la necesite, pueda acceder a ella oportunamente (esto se conoce como **Disponibilidad**).
2- Se impide el acceso a la información disponible a aquel que no tenga autorización para utilizarla. (esto se conoce como **Confidencialidad**).
3- Se evita la alteración o destrucción no autorizada de la información disponible (esto se conoce como **Integridad**).
4- Se dificulta o impide el empleo ilegal o pernicioso del espacio informativo nacional.
5- Se divulga en el exterior la verdad sobre la Revolución cubana y las amenazas o agresiones a que es sometida.

Se considera como **Espacio informativo nacional**, al *conjunto de medios y contenidos a través de los cuales se divulga información dentro de los límites del territorio nacional, así como los sitios donde se realizan actividades de información a la población, tales como: documentos oficiales; publicaciones realizadas o distribuidas en el país; vallas, carteles, plegables y otros medios de propaganda pública o de distribución individual; programas de radio y televisión, producciones cinematográficas y otros audiovisuales; redes telefónicas y de datos; sitios de Internet pertenecientes a entidades nacionales; bibliotecas, hemerotecas y videotecas públicas; espectro electromagnético y otros canales de comunicación asignados a Cuba por la OIT; así como instalaciones y otros espacios donde se desarrollen actos públicos.*

Consideramos como **Protección de la información** al *conjunto de acciones dirigidas a asegurar la integridad, la confidencialidad y la disponibilidad de la información con que el país cuenta*. Por tanto, constituye una rama o esfera de la Seguridad de la Información.

Entendemos como **Desinformación** las acciones u omisiones mediante las cuales los hechos (la verdad) se ocultan, distorsionan, descontextualizan o falsifican deliberadamente con fines ilegítimos. La desinformación se lleva a cabo por dos métodos, generalmente combinándolos:

- La **Aninformación,** o sea, la negación u ocultación de los hechos (verdades).
- La **Pseudoinformación,** o divulgación de datos y hechos falsos, descontextualizados, mutilados, distorsionados o irrelevantes, bajo la apariencia de ser verídicos, completos o relevantes, para que sean asumidos como verdadera información por los destinatarios de ella.

En referencia al empleo de la desinformación, el líder de la Revolución, Fidel Castro, ha expresado: "*…a todos nos duele la forma en que a través del control de los medios masivos de difusión, de las transnacionales de la información, nos informan lo que ellos quieren que nosotros conozcamos, y matizado de la forma que les interesa que nosotros lo conozcamos...*"[20] ,también: "*…en este mundo que llaman globalizado, donde, entre otras cosas, las más globalizadas son la desinformación y la mentira…*"[21] y recientemente "*La ausencia de la verdad y la prevalencia de la mentira es la mayor tragedia en nuestra peligrosa era nuclear*"[22]

[20] Discurso pronunciado en la clausura del III encuentro continental de mujeres, el 7 de octubre de 1988
[21] Discurso en la clausura del VII congreso de la Federación Latinoamericana de Periodistas el 12 de noviembre de 1999
[22] Reflexiones del compañero Fidel "La infinita hipocresía de Occidente" 12 de septiembre de 2010

Entendemos como **Sistema para la Seguridad de la Información**, al *conjunto de componentes que en estrecha interrelación, cumplen funciones con el objetivo de garantizar la Seguridad de la Información en el país.*

Forman parte de este sistema los siguientes componentes principales:

- La concepción
- Los documentos normativos
- Los actores
- Las acciones
- Las tecnologías de de la información
- La cultura de seguridad de la información

La **concepción** de la Seguridad de la Información se sintetiza en su definición, y cumple una función integradora y directriz de todo el sistema.

Los **documentos normativos** brindan la base jurídica para el desenvolvimiento del sistema, y cumplen una función reguladora del mismo. Incluye, entre otros, leyes, decretos-leyes, decretos, resoluciones ministeriales, normas, políticas, estrategias, y planes relacionados con el tema.

Todas las instituciones y personas que emplean información de interés para la seguridad nacional son **actores** de este sistema. Por su función pueden ser: fuentes, procesadores, custodios, administradores o consumidores de la información. Por su papel en la dirección del sistema, constituyen actores principales las siguientes instituciones: PCC, MININT, MINFAR, MIC y MINREX.

Las **acciones**, manifestadas en forma de medidas concretas que se ejecutan por los actores como parte de las propias actividades de dirección, productivas o de servicios que se desarrollan en el país, desde tiempo de paz, cumplen la función de materializar los propósitos trazados en la concepción. Incluye, entre otras, acciones de planificación, organización, gestión, coordinación, divulgación, capacitación y educación, investigación y desarrollo, legislación, control y supervisión.

Las **tecnologías** constituyen el soporte material para la obtención, reproducción, conservación y transmisión de la información en los volúmenes, calidades y plazos que el sistema requiere para su correcto funcionamiento.

La **cultura de seguridad de la información**, está integrada por valores, conocimientos, hábitos, habilidades, principios éticos, motivaciones, estilos de trabajo, y otros componentes psicosociales que condicionan el modo de actuación de los actores dentro del sistema y de este como un todo.

2.3- Riesgos, amenazas y agresiones a la seguridad de la información

Estas provienen fundamentalmente de:

- Nuestros enemigos externos y sus mercenarios internos, que de forma sistemática, planificada y con objetivos bien definidos realizan acciones de diferentes tipos.
- Personas con conductas antisociales, para la realización de actividades delictivas.
- Otras personas, por desconocimiento, negligencia, irresponsabilidad u otras razones.
- Fenómenos naturales o accidentes tecnológicos inevitables.

Atendiendo a nuestra concepción, los riesgos, amenazas o agresiones a la Seguridad de la Información pueden tipificarse en seis grandes grupos:

- ***Los relacionados con la obstaculización o limitación del acceso a la información que requiere el país, y que afecten el volumen, calidad u oportunidad con que se obtiene y emplea la misma.***
- ***Los relacionados con la posibilidad de acceso por el enemigo a información de interés para la Seguridad Nacional, con el fin de utilizarla para evaluar los potenciales de la nación, sus fortalezas y debilidades; ubicar y caracterizar objetivos políticos, económicos, sociales, científicos y militares; conocer los planes de desarrollo o de defensa de la Revolución cubana, u otros aspectos de su interés, con el fin de preparar y desarrollar acciones contra ellos.***
- ***Los relacionados con la posibilidad de destrucción o alteración de información útil y relevante, almacenada en cualquiera de sus formas, que afecte los procesos de dirección o las actividades productivas, comerciales, financieras, jurídicas, de orden interior, científicas, educacionales, culturales, militares u otras, y por tanto nuestro poderío nacional, el desarrollo sostenible del país o la defensa de la Revolución cubana, de cualquier manera.***
- ***Los relacionados con la introducción en el espacio informativo nacional, de información falsa, parcializada, mutilada, o nociva, con fines de inducir o crear en la población o determinados sectores de esta: concepciones, estados de opinión, estados de ánimo, falsos valores o modos de actuación, ajenos o contrarios a nuestros principios, o que fomenten condiciones para la aparición de fenómenos que pongan en riesgo a la Revolución Cubana***
- ***Los relacionados con el uso ilegal o pernicioso del espacio informativo nacional como plataforma para divulgar hacia el exterior información falsa o perjudicial sobre el país, para agredir los sistemas informáticos de Cuba o de otras naciones, para la subversión, o la comisión de delitos, indisciplinas sociales u otras transgresiones.***
- ***Los relacionados con la obstaculización o limitación de la divulgación en el exterior de la información sobre la Revolución cubana, sus realidades y logros, así como sobre las agresiones a que es sometida por sus enemigos y que se le oculta o se le hace llegar de forma distorsionada o falsa a la opinión pública internacional por los medios masivos de comunicación del imperio.***

Las amenazas relacionadas con la obstaculización o limitación del acceso a la información y para la divulgación hacia el exterior de la verdad sobre la Revolución Cubana, están asociadas, en primer término, a las medidas del bloqueo impuesto por los EUA a nuestro país, que le limitan la adquisición o uso de tecnologías para esta esfera y el acceso a fuentes de información en el exterior. Así mismo, se relacionan con el bloqueo mediático que intenta crear un valladar a la divulgación y conocimiento en el exterior de los logros del socialismo en nuestro país, o la ayuda solidaria a otros pueblos. También en el interior del país se manifiesta esta amenaza, vinculada a la autocensura de los medios de divulgación, los obstáculos injustificados que algunos funcionarios ponen a la labor informativa de la prensa, o como resultado de medidas supuestamente en interés de la seguridad de la información pero insuficientemente fundamentadas, cuyos efectos negativos superan con creces los beneficios que de ellas se reportan.

Las amenazas y agresiones relacionadas con la posibilidad de acceso por el enemigo a información sensible para la Seguridad Nacional, provienen, en lo fundamental, de las acciones

de la comunidad de inteligencia del enemigo, aunque no deben descartarse las acciones de espionaje industrial que puedan desarrollar compañías económicas u otras instituciones extranjeras interesadas en obtener información de desarrollos tecnológicos, negocios comerciales u otras de entidades cubanas en el marco de la competencia.

Los EUA dedican anualmente decenas de miles de millones de dólares a sufragar los gastos de su actividad de inteligencia, en busca de información en todo el mundo. Cuentan con una veintena de instituciones dedicadas a la obtención de información dentro y fuera del país, entre las que se destacan las siguientes: *Agencia Central de Inteligencia (CIA), Agencia de Seguridad Nacional (NSA), Oficina Nacional de Reconocimiento (NRO), y Buró Federal de Investigaciones (FBI).*
Las amenazas y agresiones relacionadas con la posibilidad de destrucción o alteración de información, abarcan un universo amplio de acciones u omisiones provenientes del enemigo externo, elementos antisociales nacionales, o del propio personal responsabilizado con la elaboración, procesamiento, transmisión, almacenamiento o empleo de la información. Entre estas se incluyen las siguientes:

- Destrucción de documentos en cualesquiera de sus tipos o formatos, incluido el electrónico, o de sus soportes físicos, por negligencia, error, accidente, acciones intencionales, vandálicas o de otro tipo, desastres, acción de agentes naturales (humedad, microorganismos, calor), efectos de virus informáticos, fallas técnicas y otras, sin que existan salvas o duplicados de las informaciones.
- Fallecimiento, incapacidad, abandono del país u otras, de personas en posesión de informaciones de la que tienen conocimiento exclusivo (know-how, u otros).
- Falsificación intencional de documentos oficiales con fines delictivos o contrarrevolucionarios.

Los riesgos ante estas amenazas pueden ser potencialmente altos si se toman en cuenta algunas de nuestras vulnerabilidades, como es la alta dependencia existente actualmente en las redes informáticas del uso de sistemas operativos y otros programas propietarios provenientes de Estados Unidos y otros países aliados, de los que desconocemos las instrucciones internas y puertas de acceso ocultas que puedan contener.

Las amenazas y agresiones relacionadas con la introducción en los espacios o flujos informativos de la nación, de información falsa, parcializada, mutilada o nociva, provienen esencialmente de las acciones de guerra sicológica e ideológica del enemigo. Desde el propio inicio de la Revolución, esta ha sido un arma empleada contra ella en diferentes modalidades, siendo las principales:

- La diseminación de rumores con falsedades entre la población.
- Las emisiones de radio y televisión contrarrevolucionaria
- Las introducciones clandestinas de literatura, audiovisuales y otros materiales impresos o en formato electrónico con contenidos adversos a nuestra ideología o nuestra moral, promoviendo falsos valores o la subversión contrarrevolucionaria.

Vale recordar que mediante algunos de los procedimientos anteriores, se crearon las condiciones en nuestro país para llevar a cabo la “Operación Peter Pan” que provocó la salida de unos 14 000 niños hacia los Estados Unidos entre 1960 y 1962, y los sucesos del 5 de Agosto de 1995, entre otros. En la actualidad, desde EUA se siguen emitiendo hacia nuestro país alrededor de 2300 horas semanales de transmisiones radiales y televisivas en unas 30 frecuencias.

En la actualidad, el uso ilegal del espacio informativo de carácter más peligroso se lleva a cabo, fundamentalmente, por la contrarrevolución interna y externa para su labor subversiva, y por elementos antisociales con fines de lucro.

En los últimos años ha aumentado en el mundo el peligro del delito informático en sus numerosas variantes, como pueden ser la producción y diseminación de programas malignos; el envío de "spam"; el uso de sitios Web para divulgar pornografía, mensajes fascistas, xenófobos, o racistas; la penetración de los sistemas de seguridad de ordenadores para el robo o destrucción de información, ya sea de los propios sistemas informáticos, o de los equipos o sistemas que estos controlan; el secuestro de información; el "phishing" o robo de identidades, y la estafa electrónica, entre otros. Cuba no ha estado ajena a algunos de estos fenómenos.

Por último, no puede pasarse por alto la aparición en el ámbito internacional de la concepción de la ciberguerra y otros conceptos derivados, para referirse a los actores, acciones y medios relacionados con las redes informáticas, especialmente las acciones que pueden considerarse como agresiones a las redes de datos o con el empleo de ellas, y que puedan poner en riesgo la seguridad de las naciones. Estos términos también han comenzado a utilizarse en nuestros medios de comunicación, y aunque no forman parte de nuestro aparato conceptual, por su amplio uso y significado, debemos conocerlos y ser capaces de interpretarlos.

A mediados de 2010, algunas fuentes estimaban que las llamadas "ciberarmas" formaban parte de los arsenales de unos 150 países y que treinta de ellos ya contaban con unidades de ciberguerra. Independientemente de la amenaza real que pudiera significar el empleo de estas tecnologías, a nuestro juicio lo más peligroso de este tratamiento radica en que ya Estados Unidos y la OTAN comienzan a plantear la siguiente cadena de razonamientos:

- El **ciberespacio** es un campo de batalla igual que la tierra, el mar o el aire.
- Un **ciberataque** empleando **ciberarmamento** por parte de un **ciberenemigo**, es una modalidad de ataque armado y por ello puede ser invocado el artículo 5 del Tratado de Washington (que estableció las bases para la creación de la OTAN) que considera un ataque armado contra una de sus partes, como un ataque dirigido contra todas ellas, y también el artículo 51 de la Carta de las Naciones Unidas que reconoce el derecho a la legítima defensa.
- Un **ciberataque** puede paralizar la infraestructura crítica de un país, y por tanto, poner en serio riesgo su seguridad nacional.
- A los Estados (imperialistas, por supuesto) les asiste el derecho de tomar medidas para su **ciberdefensa**, incluyendo ataques preventivos contra potenciales **ciberagresores**.

En el caso particular de los EUA destaca, por un lado, la creación de un Cibercomando para la dirección unificada de las operaciones en el ciberespacio, y por otro lado, el desarrollo de una doctrina militar que incluye, dentro del concepto de **Operaciones de información**, las **Operaciones de Redes de Computadoras** (Computer Network Operations), como uno de sus componentes, la que, a su vez, incluye tres dimensiones:

- Defensa de Redes de Computadoras
- Explotación (espionaje) de Redes de Computadoras
- Ataque a Redes de Computadoras

La aplicación de estas concepciones ya comenzó. Existen evidencias creíbles de que los primeros ataques de una nación a otra, ya se han realizado, y apreciamos puedan incrementarse en número, variedad y alcance en el futuro.

2.4- Acciones para alcanzar la Seguridad de la Información

En correspondencia con la definición de Seguridad de la Información dada, las acciones para alcanzarla pueden definirse como aquellas dirigidas a reducir los riesgos y enfrentar las amenazas y agresiones a la misma, pudiendo tener diverso carácter, incluyendo las de tipo: jurídico, organizativo, físico, técnico, educativo, y de control. Como parte de estas acciones se pueden mencionar, entre otras, las siguientes:

Acciones para garantizar la disponibilidad de la información que el país necesita para su desarrollo sostenible y para su defensa

- Desarrollo de infraestructuras de comunicaciones y redes de datos
- Desarrollo de estaciones de vigilancia meteorológica, geofísica, marítima, epidemiológica y otras
- Desarrollo de infraestructuras para la transmisión oportuna de información a la población
- Desarrollo del Sistema de Información del Gobierno
- Organización de sistemas de vigilancia tecnológica, inteligencia empresarial y equivalentes
- Realización de estudios e investigaciones científicas
- Realización de intercambios académicos
- Realización de encuestas de opinión pública nacional e internacional
- Adquisición y divulgación de libros, revistas y audiovisuales
- Inteligencia contra el enemigo externo, y contra la contrarrevolución y la delincuencia internas

Acciones para impedir el acceso a la información a personas no autorizadas

- Limitación de acceso físico a objetivos de seguridad nacional; centros, nodos y redes de comunicaciones; y locales donde se procesa o almacena la información
- Clasificación de la información
- Empleo de infraestructuras de llaves públicas, criptografía, firmas digitales y otras soluciones
- Realización de auditorías informáticas y controles a la documentación en poder de los usuarios
- Protección electromagnética
- Actividades de contrainteligencia

Acciones para asegurar la integridad de la información de que el país dispone y emplea

- Protección física contra incendios, agresión del medio ambiente, errores humanos u otras causas que puedan conllevar a la destrucción de la información.
- Desarrollo de infraestructuras de llaves públicas y otras soluciones criptográficas.
- Desarrollo y empleo de antivirus, cortafuegos y otras medidas de seguridad informática.
- Realización de salvas, reproducción de documentos en soportes duraderos, y otras medidas organizativas para su salvaguardia.
- Protección electromagnética

Acciones para impedir el empleo ilegal o pernicioso del espacio informativo nacional

- Interferencia de emisiones radiofónicas y televisivas ilegales generadas en el exterior
- Impedir la entrada y circulación de materiales impresos o audiovisuales con contenidos contrarrevolucionarios o promotores de antivalores.

- Regulación del acceso y uso del espacio informativo nacional con fines contrarios a los objetivos e intereses nacionales.
- Implementación de legislaciones para sancionar los delitos informáticos
- Incremento de las opciones informativas y de la calidad de las existentes
- Desenmascaramiento público del carácter falso o dañino de la información con estas características que logre entrar y diseminarse.

Acciones para divulgar en el exterior la verdad sobre la Revolución cubana y las amenazas o agresiones a que es sometida

- Desarrollo de programación de radio y televisión internacionales
- Desarrollo de agencias de noticias Prensa Latina y AIN
- Creación y desarrollo de redes de personalidades y otros agentes para el intercambio de información
- Discursos, entrevistas, encuentros y otras intervenciones de dirigentes y personalidades de la Revolución con cobertura de la prensa extranjera
- Desarrollo de las relaciones con los grupos de solidaridad con Cuba en el mundo
- Actividades desarrolladas por el cuerpo diplomático en el exterior
- Actividades con los corresponsales extranjeros acreditado en el país
- Publicación de sitios de Internet y desarrollo de herramientas digitales
- Fomento del turismo internacional hacia nuestro país

2.5- Relación de la Seguridad de la Información con otras dimensiones de la Seguridad Nacional

2.5.1- Relación con la Seguridad Económico Social

Varios de los riesgos que se ciernen sobre la seguridad económico-social, se derivan del bloqueo económico y financiero y de las acciones de subversión económica que ejercen los EUA contra nuestro país. Para ello, las agencias de inteligencia del imperio realizan ingentes esfuerzos en la búsqueda de información económica, sobre los socios comerciales y potenciales inversionistas extranjeros, los movimientos y estados financieros de la nación, entre otros temas; por ello, la protección de la información en estos campos, resulta esencial para defender nuestra economía.

También resultan imprescindibles las medidas de protección de la información relacionada con cambios de moneda o de sus cotizaciones internas, para evitar que individuos puedan realizar acciones con fines de lucro; así como el mantenimiento de la confiabilidad e integridad de las cuentas y los servicios bancarios, que impidan la ocurrencia de delitos financieros como desfalcos u otros.

Así mismo, al país le resulta necesario recopilar información económica, tanto del exterior, como de la economía interna, con vista a la toma de decisiones importantes en estas ramas.

Otra arista tiene que ver con el hecho de que las conductas antisociales relacionadas con el empleo de las TIC provocan pérdidas económicas al país.

En otro orden, el país dedica ingentes esfuerzos y recursos al desarrollo de la infraestructura de comunicaciones, radio y televisión, prensa escrita, instalaciones educacionales y otras que constituyen la base material que soporta el uso de la información por el país.

A la salud pública, una de sus esferas más sensibles, le es esencial la información oportuna sobre enfermedades transmisibles en el mundo, sobre la situación epidemiológica del país, o sobre

nuevos medicamentos y equipos médicos que se desarrollen en el mundo, por citar sólo algunos ejemplos, pues en otras ramas de la actividad económico-social se manifiesta igualmente la importancia de la seguridad de la información.

2.5.2- Relación con la Seguridad Político-Moral

Al analizar el contenido de las premisas que sustentan la actividad del Partido como dirigente de toda la política del país, se observa que una parte importante de ellas se refieren a actividades de obtención o divulgación de información, como son las relacionadas con el estudio a fondo de la ideología y esencia del imperialismo y en especial la forma de pensar y actuar del gobierno norteamericano, el análisis y evaluación sistemática de todas las informaciones y declaraciones que sobre Cuba se realicen, la evaluación permanente de las informaciones sobre el estado de opinión del pueblo, la denuncia ante la opinión pública de forma rápida y enérgica de cualquier agresión o infamia contra el país, para impedir que se conforme un estado de opinión falso o se creen condiciones para escaladas superiores en la política agresiva del enemigo, así como para mantener informado al pueblo de manera precisa y clara.

También, y por sus obvias implicaciones, resulta esencial la preservación de la confidencialidad sobre muchas decisiones y medidas políticas que adoptan el Partido, el Estado y el Gobierno.

2.5.3- Relación con la Seguridad Interior

Base esencial de la actividad de los órganos del Minint para prevenir y enfrentar las acciones subversivas, delictivas o antisociales de los servicios especiales enemigos, organizaciones terroristas anticubanas, grupúsculos contrarrevolucionarios, o la delincuencia, es el monitoreo permanente de sus actividades dentro y fuera del país, obteniendo información sobre sus acciones y propósitos.

La actividad de vigilancia del pueblo organizado en los Comités de Defensa de la Revolución, el sacrificado y anónimo trabajo de la agentura, el desarrollo y empleo de bases de datos sobre el potencial delictivo, o la búsqueda de indicios de contrabando en las fronteras son sólo algunas manifestaciones de obtención de información que el país necesita para su defensa, y que permiten la adopción de medidas oportunas y eficaces.

Por su parte, las acciones de los órganos de la Seguridad del Estado para contrarrestar las acciones de la inteligencia enemiga, que intenta permanentemente obtener información de interés para la seguridad nacional, también contribuyen decisivamente al logro de la Seguridad de la Información

2.5.4- Relación con la Seguridad Científico-Tecnológica

Si partimos de la definición de potencial científico y tecnológico del país como: *el conjunto de recursos humanos, **informativos**, técnicos, materiales y financieros que tienen la capacidad de producir e introducir resultados científicos y tecnológicos en aras del desarrollo*, queda claramente establecida la relación.

Por una parte, la actividad científica requiere la obtención de información sobre los objetos investigados. Por otro lado, los resultados científico-tecnológicos alcanzados, constituyen una información de gran valor y utilidad que debe ser protegida de diversas formas.

2.5.5- Relación con la Seguridad Jurídica

Para el logro de esta condición, no basta con la existencia de leyes, se requiere que la población conozca las mismas. Por ello, resulta esencial la existencia de un sistema de información jurídica organizado, que emplee los medios masivos de comunicación, el sistema educacional del país, la información personal mediante los diferentes servicios que presta el personal y las instituciones jurídicas, entre otras vías.

Por otro lado, la confidencialidad e integridad de la información que se maneja en esta esfera, es indispensable para el correcto desempeño de las funciones del sector jurídico.

2.5.6- Relación con la Seguridad Ambiental

Para asegurar la mitigación y adaptación al cambio climático, se necesita información oportuna sobre la incidencia de los problemas ambientales en el país, como: degradación de los suelos, contaminación de las aguas y la atmósfera, pérdida de la diversidad biológica y carencia de agua; con el fin de poder adoptar las medidas pertinentes de enfrentamiento.

2.5.7- Relación con la Seguridad Militar

Desde tiempo de paz, el enemigo realiza numerosas acciones de exploración contra nuestro país, con el fin de localizar la ubicación de nuestros principales objetivos militares, con vistas al empleo de sus medios de destrucción contra ellos en caso de una agresión militar. Por ello, las medidas de enmascaramiento de los objetivos y de engaño al enemigo en esta esfera, resultan de vital importancia.

Por otro lado, el país requiere también realizar una constante exploración de la actividad enemiga, con vistas a detectar a tiempo sus acciones militares y adoptar las respuestas correspondientes, evitando la sorpresa. En particular en tiempo de guerra, la exploración constituye un importante aseguramiento combativo de las FAR, que permite la localización de los objetivos del enemigo y la dirección del fuego contra ellos, así como asegura la planificación y realización de nuestras acciones combativas.

2.5.8- Relación con la Seguridad contra desastres

Fundamentalmente se relaciona con la detección y el aviso oportuno de la posible ocurrencia de fenómenos naturales o antrópicos que puedan originar la ocurrencia de un desastre, permitiendo la adopción de medidas oportunas para su reducción. En esta función juegan un papel esencial la existencia y desarrollo de redes de monitoreo meteorológico, geofísico y epidemiológico, así como también de un eficaz sistema de información a la población a través de los medios de comunicación masiva y por otras vías.

2.6- La Seguridad de la Información desde la perspectiva de la Seguridad Internacional

Los notables progresos en el desarrollo y la aplicación de las tecnologías de la información y los medios de telecomunicaciones ofrecen amplias posibilidades para el futuro desarrollo de las naciones, la multiplicación de las oportunidades de cooperación, y el aumento de la capacidad creadora de la humanidad. La comunidad internacional ha tomado conciencia de esta realidad, pero también de la posibilidad de que estas tecnologías se utilicen con propósitos que atenten contra la paz y la seguridad en el mundo, y afecten negativamente la infraestructura de los Estados.

Desde 1998 hasta la fecha, la Asamblea General de las Naciones Unidas ha aprobado una docena de resoluciones bajo el título *"Los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional"* [23], en la que se exhorta a los Estados Miembros de la organización a: "*…seguir promoviendo el examen multilateral de las amenazas reales y potenciales en el ámbito de la seguridad de la información y de posibles medidas para limitar las amenazas que surjan en ese ámbito, de manera compatible con la necesidad de preservar la libre circulación de información*" y en la que se invita a los mismos a comunicar sus opiniones sobre : "*… la evaluación general de los problemas de seguridad de la información; las medidas que se adoptan a nivel nacional para fortalecer la seguridad de la información, …las medidas que la comunidad internacional podría adoptar para fortalecer la seguridad informática a escala mundial…*"

Nuestro país no sólo ha votado afirmativamente por estas resoluciones, sino que ha enviado al Secretario General sus criterios sobre el tema, aprovechando para denunciar las constantes agresiones que en este campo sufre por parte del gobierno de los EUA.

Como principio, la política nacional en relación con la Seguridad de la Información, debe basarse en acciones que garanticen la preservación de nuestros intereses y objetivos nacionales, sin detrimento de los de los restantes Estados, y que contribuyan a los propósitos generales de las Naciones Unidas de avanzar hacia una Sociedad de la Información justa y equitativa, que contribuya al desarrollo y al bienestar de todas las naciones del planeta.

2.7- La Seguridad Informática[24], como parte componente de la Seguridad de la Información

El concepto de **Seguridad Informática** debe interpretarse como un subconjunto o parte componente de la Seguridad de la Información, y que la misma está dirigida a prevenir, detectar e impedir acciones que pongan en riesgo la disponibilidad, confidencialidad e integridad de la información tratada por los ordenadores y las redes de datos[25], pero además, el uso de estos para cometer acciones ilegales o ilegítimas, transmitir información falsa o perniciosa, o agredir las redes u otros sistemas del país o de otras naciones.

Estos conceptos, por tanto, se refieren a un soporte tecnológico específico que, por su creciente volumen de utilización y especificidades, requiere un tratamiento particular.

Se considera a la **Red de Cuba** como un *subconjunto del Espacio informativo nacional, compuesto por las redes informáticas de los órganos del estado y el gobierno, organismos de la administración central del estado, organizaciones políticas, de masas y sociales, otras instituciones y empresas, interconectadas entre sí a través de la infraestructura pública de datos*

[23] Documento A/RES/61/54 de la ONU. 19 de Diciembre de 2006

[24] En diferentes normas jurídicas cubanas y en la literatura internacional sobre estos temas se emplean, a veces como equivalentes y en otras ocasiones de manera diferenciada, los conceptos de Informática, Tecnologías de la Información, y Tecnologías de la Información (Informática) y las Comunicaciones, así como los de seguridad asociados a cada uno de ellos. En el futuro deberá llegarse a consenso entre los especialistas sobre los mismos, por lo que aquí sólo damos nuestra posición de la interpretación general que debe dárseles hasta entonces, sin intentar dar una definición acabada de estos. A los efectos de este material, emplearemos en lo adelante el concepto de Seguridad Informática.

[25] Y probablemente por otras tecnologías asociadas al uso de la información

del teleoperador nacional, que interactúan utilizando, fundamentalmente las tecnologías de Internet.

En consecuencia, la Red de Cuba constituye la parte del Espacio informativo nacional de interés para la Seguridad Informática.

2.7.1- Principales riesgos y amenazas a la Seguridad Informática

Se derivan de los riesgos y amenazas generales identificados para la Seguridad de la Información, adecuados a las particularidades de los sistemas informáticos. De modo general, estos son los siguientes:

- ***Los relacionados con la obstaculización o limitación al acceso a la información que requiere el país para perfeccionar o actualizar sus sistemas de seguridad informática.***
- ***Los relacionados con la posibilidad de acceso por el enemigo a información sensible con el fin de facilitar sus agresiones contra nuestro país, aprovechando vulnerabilidades de los sistemas informáticos, como puertas traseras, firmwares, troyanos y otros, derivados del amplio empleo de programas y equipamiento producidos en el extranjero por empresas no confiables, así como del desconocimiento o negligencias del personal que labora con información en formato digital.***
- ***Los relacionados con la posibilidad de destrucción o alteración de información útil y relevante, almacenada o transmitida por los sistemas informáticos, debido a actos delictivos de individuos, virus informáticos, fallas tecnológicas, agresión del medio ambiente, o errores humanos.***
- ***Los relacionados con el uso ilegal o pernicioso de la red de Cuba para la introducción y divulgación de información falsa o nociva; para la comisión de delitos; para la subversión; o para la agresión a las redes y ordenadores de Cuba u otras naciones, o de los equipos o sistemas tecnológicos que a través de ellos se controlan.***

Mencionaremos sólo tres ejemplos que pueden resultar aleccionadores sobre como pueden actuar los servicios especiales del enemigo en este campo, y las consecuencias que pueden tener para la seguridad nacional de un país.

- El empleo de un software que fue vendido por Canadá a la URSS, para la operación automatizada de un oleoducto, y que fue programado por los servicios de inteligencia estadounidenses para que pasado un tiempo incrementara las presiones y provocara una explosión que ocasionó enormes daños económicos a ese país.
- La venta de impresoras a Irak con un *firmware* o código oculto, que en el momento preciso fue activado para que inutilizara las computadoras de los sistemas de control de tráfico aéreo e impidiera las acciones de la fuerza aérea del país en el momento en que fue atacado por Estados Unidos y sus aliados.
- La detección en junio de 2010 de un gusano de muy complejo diseño, el Stuxnet, destinado a atacar específicamente un programa de la firma Siemens que controla instalaciones industriales, el cual parece haberse empleado con el fin de afectar las plantas de enriquecimiento de uranio en Irán, donde hubo la mayor cantidad de computadoras infectadas.

2.7.2- Principales acciones para el logro de la Seguridad Informática

Estas acciones tienen diverso carácter, tal como se enunció en el epígrafe 2.4. Si bien las acciones que a continuación se enuncian no son las únicas posibles, si consideramos que son las de mayor impacto y que no deben faltar en el diseño de ningún sistema de seguridad informática institucional:

1. Educación de los cuadros y personal en general en una cultura de seguridad informática y su preparación para trabajar en estos sistemas y enfrentar las diversas amenazas a los mismos.
2. Selección, verificación y control adecuado del personal destinado para la administración de las redes u otras responsabilidades claves.
3. Regulación del personal que tendrá acceso a las redes y del otorgamiento a este sólo de los servicios y privilegios de uso indispensables para el desempeño de sus funciones.
4. Realización sistemática de: diagnósticos remotos de vulnerabilidades de las redes; auditorías informáticas; registro, control y análisis de las trazas del uso de Internet, del correo electrónico y de otros eventos; y otros controles sorpresivos a los ejecutores.
5. Protección física de los locales donde se encuentran medios informáticos.
6. Instalación de programas autorizados de detección y eliminación de programas malignos y actualización sistemática de sus bases de datos.
7. Implementación de mecanismos de detección de intrusos o de acciones ilegales.
8. Actualización sistemática de los “parches” de seguridad para eliminar vulnerabilidades conocidas en los Sistemas operativos y aplicaciones
9. Organización y realización de salvas de la información.
10. Migración progresiva y ordenada hacia sistemas y aplicaciones de código abierto.
11. Desarrollo y uso preferente de aplicaciones informáticas nacionales.
12. Ampliación y modernización de la legislación existente, en correspondencia con los cambios tecnológicos que tienen lugar.

En particular para las entidades donde se maneje información oficial limitada o clasificada, además de las anteriores:

13. Evaluación calificada de los equipos y programas a instalar.
14. Regulaciones estrictas para la entrada/salida de los soportes con información, y para su revisión, muy especialmente los que salen del país.
15. Separación física de las redes internas de las redes con acceso a Internet.
16. Limitación de la cantidad de puntos de acceso a las redes internas y regulación de su empleo (puertos, torres de soportes magnéticos y equivalentes).
17. Reducción de los puntos de reproducción de documentos y control estricto de su empleo.
18. Clasificación de los medios y soportes informáticos, y control de su movimiento y destrucción.
19. Cifrado de ficheros que se conservan o se transmiten por las redes informáticas.
20. Implementación de medidas para el borrado seguro de la información.
21. Empleo de infraestructuras de llave pública (*cuando se implemente por el país*).

III- El empleo de la desinformación a través de los medios de comunicación masiva como un problema de seguridad nacional e internacional

3.1- Introducción

El líder de la Revolución cubana, compañero Fidel, se ha referido en varias oportunidades al uso de la desinformación como herramienta de dominación. Entre sus intervenciones podemos citar las siguientes:

"*El imperio dominó al mundo más por la economía y la mentira que por la fuerza"* [26]

"…a todos nos duele la forma en que a través del control de los medios masivos de difusión, de las transnacionales de la información, nos informan lo que ellos quieren que nosotros conozcamos, y matizado de la forma que les interesa que nosotros lo conozcamos..." [27]

"…en este mundo que llaman globalizado, donde, entre otras cosas, las más globalizadas son la desinformación y la mentira…" [28]

"*La ausencia de la verdad y la prevalencia de la mentira es la mayor tragedia en nuestra peligrosa era nuclear*" [29]

En estos juicios se percibe claramente la importancia que Fidel concede a este factor, cuyo papel en la historia, a nuestro juicio, no ha sido debidamente abordado en el campo académico.

Múltiples son los problemas de seguridad que enfrenta la humanidad en nuestros días: epidemias, guerras, grandes sismos, narcotráfico, hambre, migraciones masivas, terrorismo, piratería, deterioro ambiental, subdesarrollo económico, huracanes, corrupción, crisis económicas, crimen organizado, carreras armamentistas, políticas hegemónicas y unilaterales, entre otros.

El fenómeno que abordamos no es de nueva aparición, pero quizás hasta hace relativamente poco no había alcanzado las proporciones ni las connotaciones que hoy observamos. Al abordarlo nos proponemos demostrar que el empleo masivo de la desinformación, como herramienta de las oligarquías para el logro de sus intereses de dominación, a escala nacional o global, constituye una amenaza a la paz y un problema de seguridad internacional y nacional, y por tanto debe tratársele como tal.

---

[26] Castro Ruz, Fidel. "*Reflexiones del compañero Fidel: Las campanas están doblando por el dólar*" Diario Granma, 10 de octubre del 2009. pág. 2

[27] Castro Ruz, Fidel. "*Discurso pronunciado en la clausura del III encuentro continental de mujeres*", 7 de octubre de 1988

[28] Castro Ruz, Fidel. "*Discurso en la clausura del VII congreso de la Federación Latinoamericana de Periodistas*" 12 de noviembre de 1999

[29] Castro Ruz, Fidel. "*Reflexiones del compañero Fidel. La infinita hipocresía de Occidente"* 12 de septiembre de 2010

3.2-Desarrollo

Asumiremos como **desinformación**, las acciones u omisiones mediante las cuales los hechos (la verdad) se ocultan, distorsionan, descontextualizan o falsifican deliberadamente con fines ilegítimos. La desinformación se lleva a cabo por dos métodos fundamentales:

- La **Aninformación,** o sea, la negación u ocultación de los hechos (verdades).
- La **Pseudoinformación** o divulgación de datos y hechos falsos, descontextualizados, distorsionados o irrelevantes.

Cuando hablamos de **empleo masivo de la desinformación**, nos referimos a la que es llevada a cabo por o en interés de los grupos oligárquicos de poder, aprovechando el poder que les brindan los medios de comunicación masiva, en detrimento de una de sus tres funciones universalmente aceptadas: informar[30].

Identificamos como **medios de comunicación masiva** los tradicionalmente conocidos: la prensa escrita, la radio y la televisión; aceptando la que ya algunas fuentes comienzan a incluir, la Internet, aún cuando esta sea válida fundamentalmente en los países desarrollados donde es accesible a mayores sectores de la población, pero teniendo en cuanta que numerosos órganos de prensa, importantes televisoras e, incluso, estaciones de radio, tienen su sitio en Internet como vía alternativa para la colocación de sus mensajes, por lo que los fenómenos a los cuales nos referiremos también tienen su reflejo en la llamada "red de redes".

Cuando nos referimos a los **grupos oligárquicos de poder**, consideramos a aquellos grupos minoritarios de personas que, ya sea de derecho o de hecho, están en capacidad de influir decisivamente en la vida y en el desarrollo de las sociedades contemporáneas, haciendo uso de los poderes que su status social les confiere.

En relación con el concepto de **poder**, consideramos limitados los enfoques clásicos sobre el tema, por lo que, a los efectos de este trabajo, expondremos los que consideramos cumplen el requisito expresado en el párrafo precedente:

- **Poder económico**, ejercido por los dueños, directivos y mayores accionistas de las principales empresas e instituciones económicas y financieras, u otras personas con un significativo capital.
- **Poder político**, ejercido por los Jefes de Estado, miembros del gobierno, de los órganos legislativos, de los consejos y tribunales electorales, y los dirigentes de principales partidos políticos, tanto a nivel nacional como de los restantes niveles político-administrativos (estaduales, provinciales, municipales y equivalentes). Es válido dividirlo en **Poder ejecutivo**, **Poder legislativo** y **Poder electoral**[31]**,** puesto que en ocasiones estos sectores del poder político se enfrentan entre sí.
- **Poder judicial**, ejercido por los jueces y funcionarios en cargos importantes del aparato de justicia.
- **Poder militar**, ejercido por los mandos del ejército y la policía con unidades subordinadas, así como los de fuerzas paramilitares o irregulares armadas.

[30] Las otras son educar y entretener

[31] En algunos países el poder electoral es ejercido por el propio legislativo o por el judicial

- **Poder religioso**, ejercido por las jerarquías de las principales iglesias, pastores, predicadores y otros líderes religiosos con gran número de feligreses o seguidores.
- **Poder mediático**, ejercido por los dueños y directivos de los principales órganos de prensa, televisoras, estaciones de radio y sitios de Internet.
- **Poder popular**, ejercido por los trabajadores organizados en sindicatos, así como por otras organizaciones y movimientos sociales y territoriales, o la población en general.

Tomamos en cuenta que, con contadas excepciones históricas, el poder efectivo de las naciones ha sido ejercido por **oligarquías**, compuestas por las élites que detentan los diferentes poderes, excepto el popular (aunque en ocasiones determinados líderes sindicales, sociales o comunales han sido comprados, compulsados o engañados para aliarse a estas y atraer consigo a un sector del pueblo).

Estos diferentes grupos oligárquicos se interrelacionan y alían en una red de intereses comunes. Al respecto, Camilo Valqui y Cutberto Pastor, en su ensayo "Contribución a la crítica de la enajenación y dictadura mediática del capital imperialista" expresan*: "…los medios de comunicación de masas o mass-media, particularmente los estadounidenses, constituyen un complejo imperial que articula empresas, satélites, telefónicas, informáticas, prensa, radio, TV, campañas de publicidad, cine, autopistas de Internet, teatro y todas las sofisticadas tecnologías de comunicación. Son de propiedad de las oligarquías imperialistas que operan las finanzas, industrias, armamentos, drogas, prostitución y servicios en el mundo. Sus transnacionales, se han apoderado de todos los medios masivos de comunicación concentrándolos bajo un poder central y al mismo tiempo asegurándose el control absoluto de las nuevas tecnologías*"[32].

Esta interrelación va aparejada a una concentración y transnacionalización de los grupos mediáticos. Como afirma Ignacio Ramonet, "*estas megaempresas contemporáneas, mediante mecanismos de concentración, se apoderan de los sectores mediáticos más diversos en numerosos países, en todos los continentes, y se convierten de esta manera, por su peso económico y su importancia ideológica, en los principales actores de la mundialización liberal"*[33].

Debemos dejar claro que el uso de la desinformación no es un fenómeno nuevo ni propio del período capitalista, si bien con el desarrollo de los medios masivos de comunicación ha adquirido modalidades y connotaciones particulares.

A lo largo de los siglos estas oligarquías han utilizado la desinformación, con un **objetivo estratégico**:

- Conformar una opinión pública favorable, que apoye o al menos justifique y acepte los actos ilegítimos de esa oligarquía y el *status quo* que a esta le interesa mantener, rechace a sus adversarios, así como los cambios no deseados por ella, que estos puedan promover.

Los procedimientos utilizados para el logro de estos objetivos son diversos. En palabras de Valqui y Pastor, *"los medios masivos de comunicación mienten, demonizan, manipulan, matan,*

---

[32] Valqui Cachi, Camilo; C. Pastor Bazán. "*Capital, Poder y Medios de Comunicación: Una Crítica epistémica*" Universidad Privada Antonio Guillermo Urrelo. 2009. Pág. 34-35

[33] Ramonet, Ignacio. "*El quinto poder"*. Le Monde Diplomatique (español). 17.10.2003. Tomado de: http://www.rebelion.org/medios/031017ramonet.htm

criminalizan, ocultan el genocidio y los crímenes de lesa humanidad, encubren la colonización silenciosa, violan privacidades, falsean, envilecen, vulgarizan, caricaturizan, bastardean, intimidan, aterrorizan, provincializan, domestican y asimilan a personas, realidades, movimientos, historias, sentimientos, valores, conciencias, sentimientos y hasta diseñan y ejecutan golpes mediáticos permanentemente contra los pueblos y gobiernos que luchan contra los planes de expolio y reconquista imperialista" [34].

Nuestra proposición central es la siguiente:

El empleo masivo de la desinformación, como herramienta de las oligarquías para el logro de sus intereses de dominación, a escala nacional o global, constituye una amenaza a la paz y un problema de seguridad internacional y nacional, y por tanto debe tratársele como tal.

Los principales argumentos que sustentan esta tesis, están dados en el uso flagrante que de manera creciente y con consecuencias cada vez más peligrosas se le ha dado a la desinformación para:

1. Justificar y promover guerras de agresión, genocidios étnicos y otras formas de violencia masiva.
2. Confundir y atemorizar a la población con amenazas y riesgos inexistentes o magnificados, en lo que constituye una modalidad de terrorismo.
3. Difamar, demonizar, atacar y desestabilizar a líderes, partidos, organizaciones, organismos y gobiernos progresistas o que no responden a los interese de las oligarquías.
4. Impedir el conocimiento de la verdad sobre procesos o proyectos revolucionarios o progresistas, y sobre las agresiones que se cometen en su contra.
5. Condicionar, promover, justificar y apoyar golpes de Estado contra gobiernos constitucionales.
6. Promover o justificar la permanencia de sistemas socioeconómicos, políticas y modelos de consumo irracionales e insostenibles por la sociedad humana y el propio planeta.

Resulta obligado exponer algunos casos que contribuyan a demostrar el desarrollo histórico del uso de la desinformación y la validez de nuestra tesis central. Lo haremos siguiendo un orden cronológico, puesto que en varios de los ejemplos que utilizaremos se combinan varios de los fines anteriormente expuestos.

Muy probablemente el primer caso de empleo masivo de la desinformación con implicaciones para la seguridad internacional –casualmente con implicaciones significativas para la historia posterior de Cuba- fue la campaña desarrollada por los periódicos propiedad de William Randolph Hearst en 1898, acusando a España de la voladura del acorazado Maine en el puerto de La Habana y promoviendo una acción de los Estados Unidos contra este país. Como testimonio material quedaron los periódicos de la época y su respuesta a un corresponsal que desde La Habana le pedía que lo regresara porque aquí no había ninguna guerra: "*Quédese allí. Suminístrenos dibujos, yo le suministraré la guerra*". Si bien sería ingenuo pensar que esta campaña sensacionalista y desinformadora fue la que llevó a Estados Unidos a una guerra de rapiña que ya tenían prevista, sin dudas influyó en la opinión pública estadounidense para que

[34] Valqui Cachi, Camilo; C. Pastor Bazán. "*Capital, Poder y Medios de Comunicación: Una Crítica epistémica*" Universidad Privada Antonio Guillermo Urrelo. 2009. Pág. 58

esta justificara el posterior actuar de su gobierno que llevó a la Guerra Hispano-Estadounidense. Hearst murió hace ya mucho tiempo, pero en esencia, los métodos por él empleados aún subsisten en la prensa de ese país.

Otro caso notable tuvo como centro la Alemania nazi en el período 1929-1945, donde su Ministro de Propaganda e Información Joseph P. Goebbels, ejerciendo el control de todos los medios de comunicación, promovió el antisemitismo, el anticomunismo, el racismo y la xenofobia; ocultó sistemáticamente la existencia y finalidad de los campos de exterminio, los crímenes de guerra de sus fuerzas armadas, sus derrotas en el campo de batalla, e hizo de la mentira un arma cotidiana del nacionalsocialismo. Los principios de la propaganda que se le atribuyen, son un catálogo para el empleo masivo de la desinformación con el fin de manipular al pueblo alemán y a la opinión pública internacional de acuerdo con los intereses guerreristas y expansionistas del Tercer Reich.

Correspondientes a la década de los 50 del pasado siglo hay varios ejemplos notables. Citaremos sólo algunos, como las campañas del anticomunismo durante la llamada "guerra fría" con su expresión máxima durante la cacería de brujas del macarthismo en Estados Unidos; o las desarrolladas por diversos actores para conseguir la caída de los gobiernos nacionalistas de Muhammad H. Mossadeg en Irán, Jacobo Árbenz en Guatemala y Getulio Vargas en Brasil.

El 17 de enero de 1959, a escasas dos semanas del triunfo, el líder de la Revolución, compañero Fidel Castro denunciaba: "*…la campaña ha sido de grandes proporciones y tiene que obedecer a determinados intereses. Partió, en primer lugar, de las agencias de cables internacionales, y yo puedo dar cuenta de la mala fe con que han procedido las agencias de cables internacionales (…) han atacado, han calumniado y han llevado adelante su campaña miserable y cobarde (…) Pero ¿qué se pretende? Antes que nada: restarnos la opinión pública internacional, aislarnos*"[35]

En 1960, la Agencia Central de Inteligencia (CIA) de los EUA inició una operación de guerra sicológica contra Cuba, que se extendería por varios años, la "Operación Peter Pan", la cual se apoyó en una campaña de desinformación, en su modalidad de terrorismo mediático, sostenida por emisoras como "La Voz de los Estados Unidos" y "Radio Swan", órganos de prensa cubanos y norteamericanos, y sectores de la Iglesia católica de Cuba y los Estados Unidos. El engañoso mensaje era que el Gobierno Revolucionario promulgaría una ley por la que se retiraría la patria potestad a los padres, la que sería asumida por el Estado, el cual les quitaría los hijos desde los 5 hasta los 18 años para adoctrinarlos durante ese período, incluso enviándolos a la Unión Soviética. El resultado de esta campaña terrorista de mentiras fue la salida del país de más de 14000 niños, que tuvieron que sufrir la separación de sus familias durante años, y algunos, por toda su vida.

El control oligárquico sobre los medios de comunicación en América Latina les permitió desarrollar verdaderas guerras mediáticas contra los gobiernos progresistas de la región en los años 60 y 70, como las llevadas a cabo contra Joao Goulart en Brasil o Salvador Allende en Chile, ambas culminadas con golpes militares de consecuencias por todos conocidas.

Para atraerse a la opinión pública durante la preparación de la Guerra del Golfo en 1990, los gobiernos de Kuwait y de Estados Unidos no vacilaron en montar una farsa en la que una jovencita kuwaití contó entre llantos en el Congreso estadounidense como había visto a los

[35] Castro Ruz, Fidel. "Discurso pronunciado en Pinar del Río el 17 de enero de 1959". Periódico Granma. 17 de enero de 2009. Pág. 3

soldados iraquíes sacar de las incubadoras de un hospital de Kuwait a más de trescientos recién nacidos y tirarlos al suelo donde los dejaron morir. Esta historia fue repetida por todos los medios de comunicación, fue objeto de debate en Naciones Unidas y citada como ejemplo de la monstruosidad de Sadam Hussein por el propio Presidente George Bush. Años después se descubrió que todo había sido una gran mentira publicitaria, que el hecho nunca había ocurrido, y que la "testimoniante" era la hija del embajador de Kuwait en Estados Unidos, miembro de la familia real de aquel país y que no había estado en el lugar de los supuestos hechos.

El siglo XXI recién comienza, pero ya tiene varios ejemplos notorios.

Desde el ascenso de Hugo Chávez a la Presidencia de Venezuela en 1998, y con la paulatina radicalización de la Revolución Bolivariana por él encabezada, se produjo una creciente polarización entre los diferentes poderes de esa nación. Inicialmente, la Revolución contaba fundamentalmente con los poderes político y popular, mientras la oposición burguesa se apoyaba en los poderes económico, religioso, y mediático. El importante poder militar estaba dividido. En el 2002, los grupos oligárquicos decidieron hacer abortar el proceso revolucionario mediante un golpe de Estado. Aunque la historia de nuestra región está plagada de actos de este tipo, un elemento que singulariza este capítulo es la relevancia del papel jugado por los medios de difusión, en particular la televisión. En todo el período previo al golpe, los medios controlados por la oligarquía hicieron una feroz campaña contra el gobierno, empleando toda clase de tergiversaciones y calumnias, y, ya durante los primeros momentos del golpe, fabricando falsas agresiones contra manifestantes antigubernamentales, provocando e incitando a acciones contra el gobierno, y finalmente ocultando la reacción popular que dio al traste con el intento golpista, transmitiendo programas de entretenimiento durante esos momentos cruciales para el país.

El 20 de marzo del 2003, los Estados Unidos, con algunos aliados, comenzaron la invasión a Irak. El supuesto motivo: ese país constituía una amenaza inminente para los EUA y sus aliados, por la tenencia de armas de destrucción masiva y por sus vínculos con la organización terrorista Al Qaeda, entre otros. Durante los meses previos al inicio de la guerra, el Presidente de Estados Unidos, el Primer Ministro del Reino Unido, y el Presidente del Gobierno de España, así como otros altos funcionarios de sus gobiernos proclamaron reiteradamente la certeza del citado motivo por todos los medios de difusión y en diversas tribunas, incluida la Organización de Naciones Unidas. La campaña desinformadora alcanzó el más alto nivel jamás conocido, teniendo en cuenta las personalidades políticas de diversos Estados que la llevaron a cabo.

Resulta conveniente recordar algunas de sus intervenciones:

> George W. Bush. Presidente de EUA. Discurso el 7 de octubre de 2002 en el Cincinnati Museum Center. *"El [gobierno iraquí] posee y produce armas químicas y biológicas. El está buscando armas nucleares. El ha dado abrigo y apoyo al terrorismo…"*[36]
>
> Richard Cheney. Vicepresidente de EUA. 26 de agosto de 2002 en una Convención de veteranos de guerra: "*No hay dudas de que Saddam Hussein tiene ahora armas de destrucción masiva. No hay dudas de que las está acumulando para emplearlas contra nuestros amigos, contra nuestros aliados y contra nosotros"*.[37]

[36] "*False statements database*" The war card. The Center for Public Integrity. http://projects. publicintegrity.org/ WarCard/

[37] Lewis, Charles; M. Reading-Smith "*False pretenses*" en The war card. The Center for Public Integrity. 23.01.2003 http://projects.publicintegrity.org/WarCard/

Condolezza Rice. Asesora de Seguridad Nacional. 30 de julio de 2003 en una entrevista en "NewsHour With Jim Lehrer" del canal PBS: "*El [Saddan Hussein] tuvo armas de destrucción masiva. El las ha empleado anteriormente. El ha continuado tratando de desarrollar estos programas de armas.*"[38]

Colin Powell. Secretario de Estado EUA. Intervención ante el Consejo de Seguridad de Naciones Unidas el 5 de febrero de 2003: "*Cada afirmación que yo haga hoy está respaldada por fuentes, sólidas fuentes. No son declaraciones. Lo que les estamos dando son hechos y conclusiones basadas en sólida labor de inteligencia*".[39]

Anthony Blair. Primer Ministro del Reino Unido. Intervención ante la Cámara de los Comunes el 24 de septiembre de 2002: "*Irak posee armas químicas y biológicas (...) Sus misiles pueden ser desplegados en 45 minutos*"

José María Aznar. Presidente del Gobierno español. Comparecencia ante el Congreso de Diputados el 23 de mayo de 2003: "*Todos sabemos que Saddam Hussein tiene armas de destrucción masiva*"

Un estudio del Center for Public Integrity[40] de cuya base de datos hemos extraído algunas de las citas anteriores, reveló que entre octubre del 2001 y septiembre del 2003, sólo George W. Bush y otros siete altos funcionarios de su gobierno hicieron 935 declaraciones falsas sobre la posesión por Irak de armas de exterminio en masa y de sus relaciones con Al Qaeda.

Como se conoce nunca fueron halladas las supuestas armas, ni probados los vínculos con Al Qaeda, pero ya el objetivo estaba logrado. La fútil justificación utilizada posteriormente de que todo había sido un error de la Inteligencia sólo puede ser creído por los que carezcan de la más mínima inteligencia.

En 2009 se produce otro golpe de Estado en Latinoamérica, esta vez en Honduras. De nuevo se repite lo que ya se ha convertido en un esquema de la participación mediática:

- Fuerte campaña difamatoria previa contra el gobierno, creando las condiciones justificativas del golpe que vendrá después.
- Cierre o coacción de los medios de comunicación no plegados a los golpistas que puedan servir para denunciar el golpe en sus primeros momentos o convocar la reacción del pueblo[41].

---

[38] "*Key false statements*" The war card. The Center for Public Integrity. http://projects.publicintegrity.org/WarCard/Default.aspx?src=project_home&context=key_false_statements&id=946

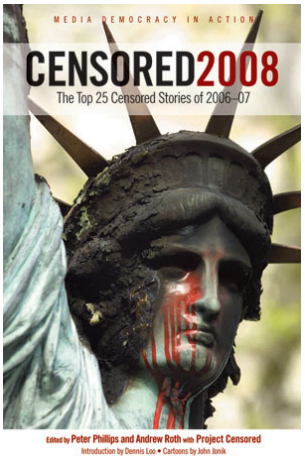
[39] "*Key false statements*" The war card. The Center for Public Integrity. http://projects.publicintegrity.org/WarCard/Default.aspx?src=project_home&context=key_false_statements&id=946

[40] The Center for Public Integrity. http://www.publicintegrity.org/WarCard/Default.aspx?src=home&context =overview&id=945

[41] En este caso a Radio Globo y al Canal 36 de noticias se les confiscaron sus equipos y se les retiraron los permisos de frecuencia radiofónicas. Pero este no es el único método. No debe olvidarse que durante el golpe de Estado al gobierno del Presidente Salvador Allende en Chile, entre los objetivos de los ataques de la aviación ese 11 de septiembre, estuvieron emisoras de radio que apoyaban al gobierno constitucional.

- Los medios al servicio de los golpistas transmiten programas de entretenimiento como si nada estuviese ocurriendo, luego edulcoran y justifican las acciones ilegales del régimen de facto y la represión contra quienes se le enfrentan, sobredimensionan los actos de apoyo al régimen, y demonizan a los que se oponen al golpe.
- Altas figuras políticas mienten sin ningún rubor ante los medios masivos de comunicación, tratando de confundir a la opinión pública sobre la realidad de los hechos.[42]

En nuestra región geográfica otras campañas desinformadoras tienen como fin desacreditar, demonizar y desestabilizar a los líderes de gobiernos progresistas como los de Venezuela, Bolivia, Ecuador, Nicaragua y Paraguay.



La divulgación de mentiras no es el único procedimiento empleado. Una de las más comunes es la aninformación, o sea la ocultación de los hechos a la opinión pública, no importa la relevancia de los mismos, siempre que el conocimiento de la verdad no convenga a los intereses de dueños del poder mediático. Los resultados publicados en Estados Unidos por el "**Proyecto Censurado**" desde 1976 hasta la fecha, dan fe de ello. El caso de nuestros cinco héroes prisioneros en cárceles de Estados Unidos es un de tantos ejemplos que pudieran citarse y que fue denunciado también por este proyecto.

Una campaña de imprevisibles consecuencias se desarrolló recientemente con toda virulencia contra Irán, tratando de crear las condiciones en la opinión pública para una posterior agresión militar contra ese país. En ella estaban presentes ambos métodos desinformativos: por un lado se silenciaron los argumentos dados por el gobierno iraní; el hecho de que Israel no es siquiera miembro del TNP, desarrolló en secreto y posee desde hace muchos años armas nucleares, y no tiene ninguna cooperación con la OIEA; y la política de doble rasero que sobre este tema desarrollan las grandes potencias; mientras que por otro lado se sobredimensionó el peligro iraní, se difamó y se demonizó a sus líderes.

La última agresión militar de Estados Unidos y la OTAN contra una nación soberana, en este caso contra Libia, tuvo su origen en la noticia de unos supuestos bombardeos del gobierno libio contra manifestantes civiles en la capital, de la cual no se dio la más mínima evidencia material, pero que luego de la consabida campaña mediática dio paso al argumento de la "necesidad de proteger a la población civil", base de la resolución del Consejo de Seguridad de la ONU que dio carta blanca a los bombardeos contra ese país.

Lo más grave es que la acción desinformadora de los medios no se circunscribe a un solo país, sino que se difunde por todo el planeta a través de las agencias de prensa, radiodifusoras y televisoras con cobertura internacional y por Internet. De esta forma, como afirma Ignacio Ramonet: *"La veracidad pasa a ser lo que todos los medios dicen que es verdad, aunque no sea cierto"*[43].

---

[42] El primer día del golpe, el usurpador Micheletti presentó una falsa carta de renuncia del Presidente Zelaya para justificar su supuesta "sucesión".

[43] Ramonet, Ignacio. *"¿Más información, más libertad?"* http://www.uned.es/ntedu/espanol/master/primero/modulos/tecnologia-y-sociedad/masinfo.htm

Algunos autores, como el propio Ramonet analizan el fenómeno adjudicándole como causa que "*…la información no tiene valor en sí misma por lo que se refiere, por ejemplo, a la verdad o a su eficacia cívica. La información es, ante todo, una mercancía y, en tanto que tal, está sometida a las leyes del mercado, de la oferta y la demanda, y no a otras leyes como, por ejemplo, los criterios cívicos o éticos*"[44]. El capitalismo, por su propia esencia, convierte y trata como una mercancía no sólo a la información, sino también a las personas, a los recursos naturales y a todo aquello que pueda brindar una ganancia, y es precisamente esta una de las facetas que lo hacen inaceptable como modelo económico-social del futuro.

Como bien apuntara el propio Ramonet, los intereses de los grandes medios de comunicación —que es equivalente a decir, de los grupos oligárquicos de poder—, no pueden "*…en ningún caso, prevalecer sobre el derecho de los ciudadanos a una información rigurosa y verificada ni servir de pretexto a la difusión consciente de informaciones falsas o difamaciones*"[45].

Existen otras modalidades más sutiles, pero no menos vergonzosas y peligrosas, que intentan ocultar o tergiversar la verdad con el uso de eufemismos como "daño colateral", "sucesión forzada", "técnicas mejoradas de interrogatorio" o "luchadores por la libertad" a lo que debiera llamarse por sus respectivos nombres: asesinato de civiles inocentes, golpe de Estado, tortura y terroristas anticubanos [46] [47] [48].

No por gusto, el tratamiento del tema Cuba en los grandes medios de comunicación también es objeto de permanente desinformación. Como ejemplos demostrativos pudiéramos citar los siguientes:

- Repetición de conceptos no ajustados a la verdad o de contenido peyorativo. Así los emigrados siempre son tratados como "exiliados", el gobierno como un "régimen" o una "dictadura".
- Ocultación o minimización de los éxitos de la Revolución, u otros que no encajan en los esquemas desinformativos establecidos sobre el país, como son los caso de los sistemas de gobierno y electoral cubanos, en relación con la imagen de "país totalitario" y "falta de democracia" que constantemente se trata de formar sobre Cuba; o la ayuda solidaria que brinda a pueblos del mundo.
- Magnificación de los problemas internos, o del papel de los grupúsculos contrarrevolucionarios. Un caso muy reciente es de una bloguera a quien se le han otorgado premios internacionales y mencionado como una de las "personalidades más influyentes" por el sólo hecho de utilizar su blog de Internet para hacer sus críticas al sistema económico y

---

[44] Ramonet, Ignacio. "*El periodismo del nuevo siglo*". La factoría No. 8, febrero 1999. http://www.lafactoriaweb.com/articulos/ramonet.htm

[45] Ramonet, Ignacio. *"El quinto poder"*. Le Monde Diplomatique (edición en español). 17.10.2003. Tomado de: http://www.rebelion.org/medios/031017ramonet.htm

[46] Artal, Rosa María. "*Eufemismos para controlarnos*" 19.08.2009 http://rosamariaartal.wordpress.com /2009/08/19/eufemismos-para-controlarnos/

[47] Núñez Betancourt, Alberto. "*Eufemismos encubren a golpistas*". Periódico Granma. 7.07.2009. http://www.granma.cu/ espanol/2009/julio/mar7/eufemismos.html

[48] Petras, James. "*Venezuela: Diccionario de eufemismos de la oposición progresista"* Rebelión. 7.1.2008. http://www.rebelion.org/noticia.php?id=61467

político cubano[49], sin olvidar los tres "Premios Sajarov" entregados por el Parlamento Europeo a "disidentes" cubanos en la actual década[50]. También al referirse al país nunca deja de mencionarse que está sumergido en una "profunda crisis económica".

- Descontextualización de los hechos para alterar la percepción y comprensión de los mismos. Un ejemplo fehaciente fue la campaña desarrollada alrededor de la detención y juicio de los cinco luchadores antiterroristas cubanos en Estados Unidos.[51]

El presidente de la Asamblea Nacional de Cuba lo recordaba en fecha reciente "…*contra Cuba el Imperio ha usado sobre todo el engaño y la falsificación de la realidad*…"[52]

Las campañas desinformadoras tienen también otro efecto no menos dañino para las personas y la sociedad en su conjunto: el de crear un clima de amenaza, desasosiego, temor e inseguridad en estas, por lo que ya algunos han comenzado a calificar las mismas como **terrorismo mediático,** calificativo justo y que compartimos. Tal como expresara el periodista brasileño Beto Almeida durante su ponencia en el Encuentro Latinoamericano contra el Terrorismo Mediático, realizado en Caracas en marzo del 2008: "*Esta degeneración comunicacional es parte de la naturaleza misma de los medios de comunicación organizados en forma de oligopólios y cada vez más como reflejo de la inevitable concentración del sistema capitalista*"[53]. En ese mismo encuentro Vicente Romano apuntaba "*La manera más efectiva para ocultar los actos de violencia psicológica y física de un sistema social que genera angustias, incertidumbre por el futuro, precariedad en el empleo, discriminación de todo tipo, etc., es crear un discurso que mantenga el miedo y haga creer a la población que no hay otra alternativa que la resignación. Es decir, el discurso de la mentira y del engaño"*[54]

Ocultar la verdad o impedir su divulgación, difundir mentiras y cuasi-mentiras (término más apropiado que el de "verdades a medias"), no debe seguirse viendo como un simple problema de falta de ética periodística o política. Es una agresión tanto a las personalidades, o instituciones que se atacan, como a los millones de personas que conforman el público, a quien se le priva del conocimiento de la verdad.

Este tipo de acciones viola preceptos incluidos en los artículos 19 y 20 del Pacto Internacional de derechos civiles y políticos, donde se plantea que el derecho a difundir informaciones e ideas de toda índole entraña deberes y responsabilidades especiales y por tanto estará sujeto a ciertas

---

[49] Algunos llegan a límites de ridículo, como el de "Héroes del Hemisferio" otorgado por la Fundación Panamericana del Desarrollo.

[50] A Oswaldo Payá (2002), las Damas de Blanco (2005) y Guillermo Fariñas (2010)

[51] Esto en combinación con un silencio casi absoluto en la prensa norteamericana de las flagrantes arbitrariedades judiciales cometidas a lo largo de todo el proceso

[52] Alarcón de Quesada, Ricardo. Palabras de clausura en el Encuentro de Cubanos Residentes en el Exterior, Contra el Bloqueo y en Defensa de la Soberanía Nacional. Periódico Granma 30.1.2010 pág. 5

[53] Almeida, Beto. "*Terrorismo mediático y unidad latinoamericana"*. Ponencia presentada al panel "Imperialismo y Unidad Sudamericana", en el Encuentro Latinoamericano contra el Terrorismo Mediático. Caracas. Marzo 2008. http://www.rebelion.org/ noticia.php?id =65613

[54] Romano, Vicente. "*Libertad de expresión y terrorismo mediático"* Ponencia expuesta en el Encuentro Latinoamericano contra el Terrorismo Mediático. Caracas. Marzo 2008 http://www.rebelion.org/noticia.php?id=66104

restricciones, que deberán estar expresamente fijadas por la ley y sean necesarias para asegurar el respeto a los derechos o a la reputación de los demás, y la protección de la seguridad nacional, el orden público o la salud o la moral públicas. Así mismo, expresa que toda propaganda en favor de la guerra estará prohibida por la ley[55].

La periodista argentina Estella Calloni afirma: *"Ahora la palabra mata, oculta crímenes brutales bajo envolturas de mensajes muy bien preparados"*[56]*;* Ignacio Ramonet expresa: "*Vivimos en un estado de inseguridad informativa*"[57]; mientras que Valqui y Pastor sentencian que: "*Las técnicas y reglas de la propaganda, la desinformación, la censura, la masificación del engaño y la guerra psicológica, son las armas básicas de las actuales guerras imperialistas estadounidenses que los mass media las reproducen en escala ampliada*"[58].

Esta es la realidad que vivimos a diario, pero no la que queremos para vivir. Tampoco debemos conformarnos con la impunidad de los que ocultan deliberadamente la verdad, tergiversan los hechos según sus intereses o mienten deliberadamente a la opinión pública. Urge pues actuar para cambiar también al mundo en lo que a tratamiento de la información se refiere.

Si una empresa productora o comercializadora de alimentos saca al mercado productos adulterados o contaminados, violando las leyes sanitarias, que provoquen trastornos o enfermedades a los consumidores, seguramente sus directivos serían demandados, encausados, y condenados por ello.

Los seres humanos nos hemos diferenciado del resto del mundo animal por nuestra capacidad de procesar racionalmente la información que recibimos, y constantemente estamos tomando decisiones de todo tipo en base a esa información, y por tanto esta nos resulta un recurso vital, entonces. Entonces, a quienes deliberadamente nos priven de información importante o nos intoxiquen con información adulterada o contaminada debiera dárseles similar trato a quienes lo hacen con el agua que bebemos, los alimentos que comemos o el aire que respiramos.

Iniciativas como el Observatorio Internacional de Medios de Comunicación promovido por Ignacio Ramonet con el que pretende ejercer un contrapeso moral al poder mediático, sancionando sus faltas de honestidad a través de informes y estudios que elabora, publica y difunde[59], tal como hace con sus "Perlas informativas" el periodista Pascual Serrano en el medio alternativo "Rebelión", o los artículos de prensa y denuncias de periodistas y otros intelectuales honestos, son loables pero insuficientes.

Debe tenerse en cuenta que en la actualidad, el fenómeno del empleo masivo de la desinformación no es espontáneo ni fruto de acciones irresponsables de individuos aislados.

---

[55] ____ Pacto Internacional de Derechos Civiles y Políticos, A.G. res. 2200A (XXI), 21 U.N. GAOR Supp. (No. 16) p. 52, ONU Doc. A/6316. 1966

[56] Calloni, Stella. "*La información como arma de guerra: la palabra que mata*". 23.07.2007. http://www.cubadebate.cu/opinion/2007/07/23/la-informacion-como-arma-de-guerra-la-palabra-que-mata/

[57] Ramonet, Ignacio. Citado por Hidalgo, Mariló. "*Los medios de comunicación y el negocio de la guerra*" http://www1.umn.edu/humanrts/instree/spanish/sb2esc.html

[58] Valqui Cachi, Camilo; C. Pastor Bazán. "*Capital, Poder y Medios de Comunicación: Una Crítica epistémica*" Universidad Privada Antonio Guillermo Urrelo. 2009. Pág. 50

[59] Ramonet, Ignacio. *"El quinto poder"*. Le Monde Diplomatique (español). 17.10.2003. Tomado de: http://www.rebelion.org/medios/031017ramonet.htm

Como ha sido documentado por diversos autores[60] [61], es el resultado de la acción coordinada de una red de instituciones de diverso carácter: financieras, de inteligencia, asociaciones de dueños de periódicos, ONG's, "*think tanks*", grupos empresariales y otras muy diferentes en su forma, pero con un objetivo de clase común.

Se requiere la adopción de legislaciones nacionales que aseguren la democratización efectiva de los medios masivos de comunicación y sancionen el uso inescrupuloso e ilegítimo de los mismos para defender mediante la mentira y el engaño los intereses de las oligarquías que históricamente han detentado el poder. Así mismo se requiere la negociación de instrumentos internacionales con igual fin.

Ya algunas naciones de nuestro continente, como Argentina, Ecuador y Venezuela, se han planteado la necesidad de adoptar leyes que sancionen esta práctica espuria, y dan los primeros pasos en esa dirección, pero los "latifundios de la información" como los ha llamado Gérard Devienne[62], continúan siendo predominantes en casi todo el planeta.

3.3- Conclusiones

Parte de lo que hemos expuesto anteriormente ya ha sido denunciado en múltiples foros y medios alternativos, por reconocidos intelectuales y periodistas. Aún cuando no resultara del todo novedoso, consideramos justo aprovechar toda tribuna posible para profundizar en el tema y hacer conciencia sobre ello. Sin embargo, lo que aún no se había dicho explícitamente, es la conclusión a la que hemos arribado como resultado del estudio de los diferentes enfoques dados por otros autores, y que consideramos la proposición central de esta exposición: **el empleo masivo de la desinformación, como herramienta de las oligarquías para el logro de sus intereses de dominación, a escala nacional o internacional, constituye una amenaza a la paz y un problema de seguridad internacional, y por tanto, debe tratársele como tal**.

Si las guerras imperiales, golpes de Estado contra gobiernos democráticos, guerras civiles u otras acciones violentas, tienen desastrosas consecuencias de muertos y heridos, destrucción de la infraestructura del territorio, desplazamiento e inseguridad de la población, muchas de ellas irreversibles, entonces realizar campañas desinformadoras con el fin de justificarlas o alentarlas es tan condenable como estas propias acciones, y los individuos, instituciones y medios de comunicación que sean partícipes de las mismas deben ser considerados una amenaza para la paz, violadores del derecho internacional y sancionados por ello.

Si el terrorismo, en todas sus formas, se considera un flagelo para la humanidad que debe ser combatido con firmeza, entonces quienes desarrollen campañas desinformadoras con el fin de atemorizar a la población, crear situaciones de inestabilidad y conflictos con los gobiernos, u otras modalidades de terrorismo mediático, deben ser considerados terroristas, violadores del derecho internacional y sancionados por ello.

---

[60] Golinger, Eva. *"El terrorismo mediático, las operaciones psicológicas, la SIP y la necesidad de un movimiento internacional de comunicación revolucionaria"* Rebelión. 2.4.2008. http://www.rebelion.org/noticia.php?id=65444

[61] Bleitrach, Danielle; V. Dedal; M. Vivas. "*Estados Unidos o el imperio del mal en peor*". Editorial José Martí. 2006 Pág. 155-185

[62] Devienne, Gérald. "*Los latifundios de la información*" Rebelión. 04.08.2009 http://www.rebelion.org/noticia.php?id=89567&titular=los-latifundios-de-la-información

Si a la luz del derecho internacional, y tal como recogen múltiples códigos penales nacionales, la difamación es un delito, quienes con fines ilegítimos empleen los medios masivos de comunicación para realizar campañas de mentiras contra líderes sociales, procesos políticos, organismos e instituciones nacionales e internacionales, deben ser considerados criminales y sancionados por ello.

Si los seres humanos necesitan de la información tanto como del oxígeno, el agua o los alimentos, es tan delito privarlos de una como de los otros, y es tan criminal contaminar la información con mentiras, como contaminar el medio ambiente. El derecho al conocimiento de la verdad, resulta vital para el correcto desenvolvimiento de las personas, grupos humanos y la sociedad en su conjunto, por lo que negársela o falseársela con fines ilegítimos es un acto que debe ser condenable no sólo ética sino también jurídicamente.

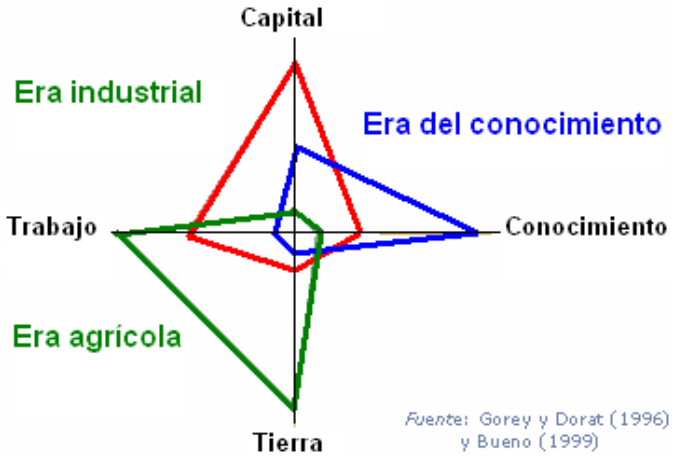
Se requiere hacer conciencia sobre el peligro que representa para la humanidad que una élite de poder inescrupulosa utilice a su antojo la mentira y la ocultación de la verdad para el logro de sus fines. Hay que alertar y educar a los pueblos para que conozcan los procedimientos de desinformación que se emplean contra ellos.

Más aún, se requiere la negociación y aprobación de un instrumento internacional que sancione el empleo masivo de la desinformación para fines ilegítimos que pongan en riesgo la paz y la seguridad internacional.

IV- El desarrollo de la informática y las comunicaciones y la Sociedad de la información. Oportunidades y amenazas para la Seguridad nacional

Profundos avances en ramas como la microelectrónica, la informática, las telecomunicaciones y los procesos de digitalización de señales, unidos a la acumulación del saber alrededor de estos temas, propiciaron a finales de los años 90 del pasado siglo una convergencia de tecnologías hasta aquel momento independientes, las cuales en un proceso acelerado de convergencia impactan en todos los aspectos de la sociedad humana. El trabajo, la escuela, el hogar, el entretenimiento, entre otros, no escapan al efecto cada vez mayor de estas tecnologías en todos los aspectos de la vida, lo que conlleva a un fuerte vínculo de las mismas con los cambios económicos, políticos y sociales de nuestra época. Ellas, sin ser un fin en sí mismas, son herramientas que propician el cambio y la modernización en todas las esferas sociales en que se insertan, de manera ubicua e integradora, donde su uso intensivo facilita mayor inserción e intercambio generalizado entre los sistemas que interactúan y promueven mayor nivel de bienestar y calidad de vida.

En consecuencia, se habla de la "Sociedad de la Información" para caracterizar el momento histórico actual y algunos autores predicen ya el futuro advenimiento de la "Sociedad del Conocimiento". Un precepto queda bien claro; la información es vital como materia prima, pero transformarla en conocimiento requiere mucho más.[(63)]



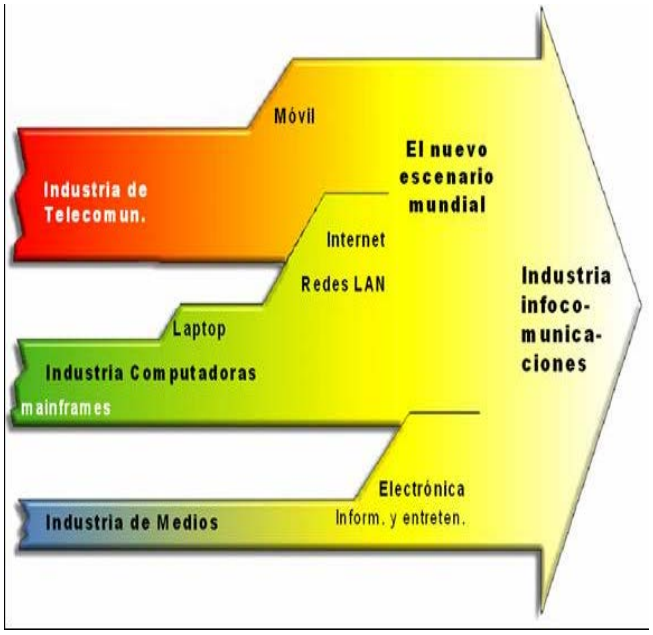
El panorama económico mundial ha cambiado dramáticamente en los últimos dos siglos, pasando desde una sociedad en general agrícola, a través de la sociedad industrial hacia la sociedad de la información en estos tiempos; pero manteniendo amplísimas brechas en los niveles de desarrollo de cada país y dentro de estos, entre los diferentes sectores sociales.

[63]El Dr. Ismael Clark, Presidente de la ACC, considera que "el conocimiento ha sido uno de los términos mercantilizados en esta época: se habla de industria del conocimiento e (incluso) de gerencia del conocimiento, como si el conocimiento fuera algo susceptible de comercializarse, con independencia del sujeto que posee ese conocimiento; se le trata como una cosa, algo que existe y puede colocarse en portadores digitales o sitios de Internet. En propiedad, tales cosas debieran identificarse como datos o incluso como información, pero el concepto de conocimiento hay que reservarlo para aquella información que es contextual e históricamente situada por un sujeto conocedor". (Clark, I. 2007)

Se considera que la primera convergencia tecnológica comenzó en la década del 60 del pasado siglo, cuando el explosivo crecimiento de la capacidad de procesamiento se aplicó a los equipos de telecomunicaciones y se acompañó de un sostenido desarrollo de la microelectrónica y la fotolitografía.

La "Ley de Moore", que relaciona la capacidad de cómputo con la cantidad de transistores presentes en un procesador en el tiempo, ilustra este fenómeno al asegurar que se duplica la capacidad de cómputo cada año.

La denominada segunda convergencia tecnológica ocurrida en los años 90 del siglo XX y mencionada al inicio de este material, catalizó, de alguna forma, el significativo proceso de Globalización que detonó a finales del pasado siglo.



Un nuevo término; "Tecnologías de la Información y las Comunicaciones" (TIC), quedó acuñado, intentando en su acepción agrupar todos los elementos y técnicas utilizadas en el tratamiento, almacenamiento y transmisión de señales, como manifestación física de ese importante recurso que es la información.

El acelerado desarrollo de la ciencia y la tecnología como importantes fuerzas productivas del mundo contemporáneo revela el importantísimo papel transformador del conocimiento. Su transformación cualitativa, más que su acumulación cuantitativa, abre nuevas perspectivas para un posible desarrollo social y económico sustentable.

En tal sentido, la capacidad de una nación de dominar las TIC, es reconocida como un factor crítico para su desarrollo económico y social, además de influir directamente en su capacidad de defensa en tanto se relaciona directamente con aspectos específicos de la Seguridad Nacional.

En el 1994 ocurre el despegue internacional de Internet, la conocida "red de redes", seguida pocos años después por la tecnología de Internet inalámbrica; la **movilidad** como característica del uso (tanto en la computación, las telecomunicaciones como en los medios) se pone de manifiesto, y lo que en su momento se conoció como una evolución digital se convierte en una revolución digital: aparecen sofisticados dispositivos que integran en un mismo cuerpo funcionalidades diversas de comunicación, computación, contenidos multimedia, que implican el inicio de la desaparición de las tradicionales fronteras entre equipos electrodomésticos, computadoras y equipos de comunicaciones (por mencionar sólo unos cuantos).

Este hecho es posible a partir de que los datos – en su acepción amplia – se representan en un mismo lenguaje: ceros o unos, verdadero o falso, existencia o no de energía, lo que permite resolver diferentes funciones con un mismo tipo de dispositivo electrónico.

Caracteriza esta convergencia tecnológica una propiedad: la velocidad.

Si la radio como tecnología se demoró 74 años para alcanzar sus primeros 50 millones de usuarios, Internet como tecnología necesitó sólo 4 años.

Todo este proceso está confluyendo hacia una tercera convergencia tecnológica, a partir de la sinergia que está ocurriendo entre la informática, la nanotecnología, las ciencias cognitivas y la biotecnología (representadas por los bits, los átomos, las neuronas y los genes), lo cual presupone otro salto acelerado en el desarrollo, con los riesgos intrínsecos que le acompañan, al generar la percepción de la necesidad de cambiar tecnológicamente sin haber asimilado totalmente los conocimientos de etapas previas, y en la cual la brecha existente entre los países explotadores más desarrollados y los países históricamente explotados se ensancha cada vez más.

Ese proceso impulsado por la aparición de tecnologías cada vez más novedosas que responden a marcados intereses de los gobiernos de los países que las producen, debe acompañarse ineludiblemente de nuevos modelos y nuevas capacidades para su utilización, de forma tal que podamos apropiarnos de las mismas y utilizarlas en beneficio del desarrollo sostenible de nuestros países.

Una consultora internacional, Gartner, identificó a finales de 2010 las 10 tendencias principales del desarrollo de las TIC para el 2011:

1. **Computación en "nube"**- Se ofrecen servicios informáticos a través de internet sin que el usuario final tenga que conocer dónde se encuentran los mismos.
2. **Aplicaciones para dispositivos móviles**- El avance de la tecnología con movilidad implica una alta demanda de aplicaciones para estos dispositivos
3. **Comunicación y colaboración social**- La irrupción del denominado "software" social y de las redes sociales, como fenómenos de ordenamiento en la red para trabajar de manera dinámica a lo largo de una organización, han tenido una amplia repercusión en el uso entre personas de diferente procedencias de servicios como "Facebook" o "Twitter".
4. **Uso del video**- En sí mismo no resulta una novedad, sino la tendencia a una muy alta presencia del video en todo tipo de gestión de contenidos.
5. **Nueva generación de sistemas de análisis y monitorización**- Uso de herramientas de análisis para simular y mejorar los procesos de una estructura y lograr más eficacia en la toma de decisiones.
6. **Análisis y monitorización social**- Similar al caso anterior, pero utilizada para simular el comportamiento de grupos humanos.
7. **Computación atenta al contexto**- Se logran en la "nube" espacios separados para el usuario: contexto público, contexto empresarial y contexto doméstico.
8. **Sistemas de almacenamiento y memoria accesible**- No sólo el uso, ya muy extendido, sino la alta capacidad de almacenamiento y los dispositivos que funcionan basados en esta tecnología (reproductores de medios, discos duros sin partes en movimiento).
9. **Computación ubicua**- Es una derivación de la computación atenta al contexto, en cuanto al modo de utilización.
10. **Sistemas e infraestructura entrelazada**- Un sistema puede agregarse a partir de bloques independientes, que se montan sobre sistemas mínimos comunes ya fabricados; el modelo abstrae la infraestructura física concreta en un "pañol" de recursos que es manejado convenientemente por el software especializado.

Todas las oportunidades que estos fenómenos pueden brindar para una mayor eficiencia de los procesos que se desarrollan en las diferentes esferas de una sociedad, sobre todo en los procesos asociados a la toma de decisiones de manera oportuna, están matizadas a su vez por un escenario internacional que puede caracterizarse con algunos datos de la manera siguiente:

- aunque hubo un decrecimiento en el 2009 con relación al 2008 de los gastos en tecnologías de la información a escala global, está previsto un crecimiento de los mismos en 2010 con relación a 2009, siendo el área de telecomunicaciones la de mayor gasto, seguida de los servicios en TI, el equipamiento (*hardware*) y los sistemas y aplicaciones informáticas (*software*), en ese orden;
- dentro del gasto en telecomunicaciones se aprecia un crecimiento en la cantidad de suscriptores de servicios de banda ancha, se mantiene el sustancial crecimiento en líneas móviles y comienza a decrecer lentamente el servicio fijo;
- el crecimiento acumulado en gastos de I+D de las principales compañías TIC entre 2000 y 2006 es mayor en Taiwan, seguido de China, Corea del Sur, Alemania, EE.UU., Japón y Francia; aunque entre 2008 y 2009 los EE.UU realizaron el 40% de todos los gastos en I+D realizados por los países de la OCDE en la industria manufacturera y de servicios de las TIC;
- en particular en sistemas y aplicaciones informáticas (*software*), EE.UU. invierte cerca de 30 mil 500 millones USD, seguido de Israel (2 mil 500 millones), Japón y Reino Unido (2 millones cada uno) y Alemania (1,9 millones);
- algunas economías que no son miembros de la OCDE se están convirtiendo en importantes inversores en I+D en las TIC;
- la mayor cantidad de computadoras personales por personas están en América del Norte, seguidos de Europa occidental, Europa del este y Rusia, América Latina, Asia y Australia y finaliza con Oriente medio y África;[64]
- grandes consorcios del mundo informático apuntalan con sus aplicaciones las redes sociales, pero con el apoyo de varios servicios de inteligencia que monitorean lo que ocurre en las mismas;
- las sistemas y aplicaciones informáticas en código abierto (*"software libre"*) continúan ampliando su radio de utilización, acompañadas por algunas conversiones a esquemas propietarios de aplicaciones anteriormente "libres" a partir de adquisiciones, (como ocurrió con el gestor de bases de datos MySQL que fue adquirido por Oracle Corporation);
- avanza a menor velocidad de lo esperado la incursión hacia la televisión digital y varios países de América Latina seleccionan la norma brasileño-japonesa SBTVD como estándar para las transmisiones, debido a sus bondades en la interactividad;
- avances en la microelectrónica permiten altas velocidades de procesamiento, así como lograr dispositivos en la escala de 25 nanómetros, lo cual es el tamaño de determinados virus (a manera de ejemplo, el grosor de un cabello humano está en el orden de los 90 mil nanómetros).

Lo cierto es que, desde 1993, en que la administración estadounidense de Clinton-Gore lanzó la idea de la Infraestructura Nacional de la Información (*National Information Infrastructure – NII*) hasta nuestros días, no han cesado de ponerse en práctica, ya con alcance local, regional, nacional o mundial, diversas iniciativas que persiguen impulsar el avance hacia la denominada Sociedad de la Información.

64 La división en regiones es la utilizada por la fuente "Economist Intelligence Unit"

También en 1993 Japón aborda el tema a través del Consejo de Telecomunicaciones y comienza el desarrollo de la infraestructura de fibra óptica para unir las islas que conforman ese país.

Los propios Estados Unidos buscando la hegemonía en el control de la información que circula a través de las redes propone en un encuentro de la Unión Internacional de Telecomunicaciones (UIT) celebrado en Buenos Aires en 1994, la creación de una Infraestructura Global de la Información (GII).

Ese mismo año, la vicepresidencia de la Comisión Europea emitió un "Informe sobre la sociedad de la información", conocido como Reporte Bangemann[65], que sostenía que se podrá "tratar, almacenar, encontrar y comunicar informaciones en cualquiera de sus formas (oral, escrita, en imágenes, etc.) sin límites de tiempo, espacio y volumen" y que aborda los principios y proyectos fundamentales que han de caracterizar un proceso ordenado de informatización desde la perspectiva social (salud, educación, entre otros ámbitos).

En los años 1995 - 96, se dan pasos que permiten fundamentar mejor el concepto de las Autopistas de la Información, las Redes de alcance global y otras iniciativas que se ven materializadas en diferentes foros internacionales como la Conferencia de Telecomunicaciones de la ONU, la Reunión Ministerial especial del Grupo de los 7 (G7), en Bruselas, en el Proyecto Autopista de la Información en Canadá y en la iniciativa de la Sociedad de la información africana (AISI), pasando por la publicación en 1997 del “Marco para el Comercio Electrónico Global” por los Estados Unidos, existiendo desde entonces el riesgo de la privatización de la "red de información planetaria" preconizada en Bruselas.

Un hito en estos escenarios lo constituye la celebración de la Cumbre Mundial sobre la Sociedad de la Información (CMSI), organizada por las Naciones Unidas y celebrada en 2 fases: Ginebra 2003 y Túnez 2005.

La “Declaración de Principios” de esta Cumbre, en relación con el concepto “sociedad de la información” describe:[66]

“A-Nuestra visión común de la sociedad de la información

*1-**Nosotros, representantes de los pueblos del mundo, reunidos en Ginebra del 10 al 12 de diciembre de 2003 con motivo de la primera fase de la Cumbre Mundial sobre la Sociedad de la Información**, declaramos nuestro deseo y compromiso comunes de construir una sociedad de la información centrada en la persona, incluyente y orientada al desarrollo, en la que todos puedan crear, consultar, utilizar y compartir la información y el conocimiento, para que las personas, las comunidades y los pueblos puedan desarrollar su pleno potencial en la promoción de su desarrollo sostenible y mejorar su calidad de vida, de acuerdo con los objetivos y principios de la Carta de las Naciones Unidas y respetando y defendiendo plenamente la Declaración Universal de Derechos Humanos.”*

y más adelante señala:

“B-Una sociedad de la información para todos: principios fundamentales

[65] Por ser Martín Bangemann el coordinador de un grupo constituido por 20 miembros de alto nivel encargados de establecer los lineamientos necesarios para el desarrollo de la Sociedad de la Información en los países europeos,

[66] Documento WSIS-03/GENEVA/DOC/4-S, “Declaración de Principios”, diciembre 2003

*19-**Estamos decididos** a proseguir nuestra búsqueda para garantizar que todos beneficien de las oportunidades que puedan brindar las TIC. Convenimos en que, para responder a tales desafíos, todas las partes interesadas deben colaborar para acrecentar el acceso a la infraestructura y las tecnologías de la información y la comunicación, así como a la información y al conocimiento, crear capacidades, propiciar la confianza y la seguridad en cuanto a la utilización de las TIC, crear un entorno habilitador a todos los niveles, desarrollar y ampliar las aplicaciones TIC, promover y respetar la diversidad cultural, reconocer el cometido de los medios de comunicación, abordar los aspectos éticos de la sociedad de la información y alentar la cooperación internacional y regional. Acordamos que éstos son los principios fundamentales de la construcción de una sociedad de la información para todos."*

El propio documento indica en 11 acápites hacia dónde dirigir los principales esfuerzos:

1.- La función de los gobiernos y de todas las partes interesadas en la promoción de las TIC para el desarrollo
2.- Infraestructura de la información y la comunicación: fundamento básico de una sociedad de la información para todos
3.- Acceso a la información y al conocimiento
4.- Creación de capacidades
5.- Crear confianza y seguridad en la utilización de las TIC
6.- Entorno habilitador
7.- Aplicaciones de las TIC: ventajas en todos los aspectos de la vida
8.- Diversidad e identidad culturales, diversidad lingüística y contenido local
9.- Medios de comunicación
10.- Dimensiones éticas de la sociedad de la información
11.- Cooperación internacional y regional

y se expresa:

- *"5) Crear confianza y seguridad en la utilización de las TIC"*

35-Reforzar el marco de confianza que abarca, entre otras cosas, la seguridad de la información y la seguridad de las redes, la autenticación, la privacidad y la protección de los consumidores, es requisito previo para que se desarrolle la sociedad de la información y promover la confianza de usuarios en las TIC. Se debe fomentar, desarrollar y poner en práctica una cultura mundial de la ciberseguridad en cooperación con todas las partes interesadas y los organismos internacionales especializados. Habría que respaldar dichos esfuerzos con una mayor cooperación internacional. Dentro de esta cultura mundial de la ciberseguridad, es importante mejorar la seguridad y garantizar la protección de los datos y la privacidad al tiempo que se mejora el acceso y el comercio. Por otra parte, es necesario tener en cuenta el nivel de desarrollo social y económico de cada país, así como los aspectos de la sociedad de la información relacionados con el desarrollo.

36-Si bien se reconocen los principios de acceso universal y sin discriminación a las TIC para todas las naciones, apoyamos las actividades de las Naciones Unidas encaminadas a impedir que se utilicen estas tecnologías con fines incompatibles con el mantenimiento de la estabilidad y seguridad internacionales, lo que podría menoscabar la integridad de las infraestructuras nacionales al atentar contra seguridad ...)"

Sin embargo, desde la propia campaña electoral de Clinton, cuando su designado Vicepresidente, Albert Gore, tomó como bandera el desarrollo de la "autopista de la información", "tanques pensantes" de EE.UU. estudiaron la viabilidad de llevar los bits al campo de batalla y se expusieron conceptos como el de ciberguerra. Con George W. Bush y los acontecimientos del 11 de septiembre estas concepciones recibieron un nuevo impulso, Rumsfeld declara que "*Internet es el nuevo escenario de la guerra contra el terror*" y se desata una campaña que dura hasta nuestros días. Barack Obama crea la figura del Ciberzar, quien coordina los esfuerzos para mejorar la ciberseguridad en el ámbito militar y civil; designa al frente al ex-director de Seguridad Nacional; activa el cibercomando, con más de 80 000 efectivos y la misión de desarrollar acciones de ciberguerra.

La propia globalización a la que estas tecnologías están sujetas impone determinados retos a todos los países:

- se utilizan los mismos sistemas operativos y aplicaciones básicas, que se han constituido en estándares internacionales *de facto*;
- existen vulnerabilidades en los sistemas operativos y las aplicaciones;
- ocurren ataques en forma de programas malignos, desfiguración de sitios web, correos basura, redes zombies[67], entre otros.

Por otra parte, los EE.UU. busca desde hace varios años lograr la supremacía en el control de la información, lo que a su vez impulsa a otros países fundamentalmente de la Unión Europea a entrar en una carrera similar.

Durante la década de los 90 se produce un gran número de estudios por institutos de investigación y "tanques pensantes" de los Estados Unidos sobre la viabilidad de llevar los bits al campo de batalla; uno muy renombrado fue el desarrollado por dos especialistas en conflictos en la era de la información, John Arquilla y David Ronfeldt, "*The Emergence of Noopolitik: Towards an American Information Strateg*y", en el que exponen un grupo de conceptos como: ciberguerra (*cyberwar*), guerra en red (*netwar*) y política del conocimiento (*noopolitic*). Estos investigadores, el primero de ellos ex marine del ejército estadounidense, planteaba que "la revolución de la información altera la naturaleza de los conflictos e introduce nuevas modalidades de guerra, el terrorismo y el crimen", otros caracterizan a la época actual "por un desplazamiento en la relación entre lo tangible y lo intangible en los métodos tanto de producción como de destrucción". Joseph S. Nye, asistente del Secretario de Defensa de la Administración Clinton, planteó durante su mandato que "El país que mejor sepa conducir la revolución de la información será el más poderoso... Y en el futuro previsible, ese país será Estados Unidos", añadiendo que "al igual que la supremacía nuclear era la clave para el liderazgo de la coalición en el pasado, la supremacía informativa será la clave en la era de la información".

Con el advenimiento de la administración de George W. Bush y los acontecimientos del 11 de septiembre de 2001, estas concepciones recibieron un nuevo impulso, el entonces Secretario de Defensa, Donald Rumsfeld, declara que "Internet es el nuevo escenario de la guerra contra el terror". En el año 2004 se crea por parte de la Rand Corporation el concepto de ASAP (Análisis y procesamiento de Señales Atípicas), que debía permitir a la comunidad de inteligencia conectar puntos para de una forma rápida identificar e interpretar pistas, "una búsqueda de información

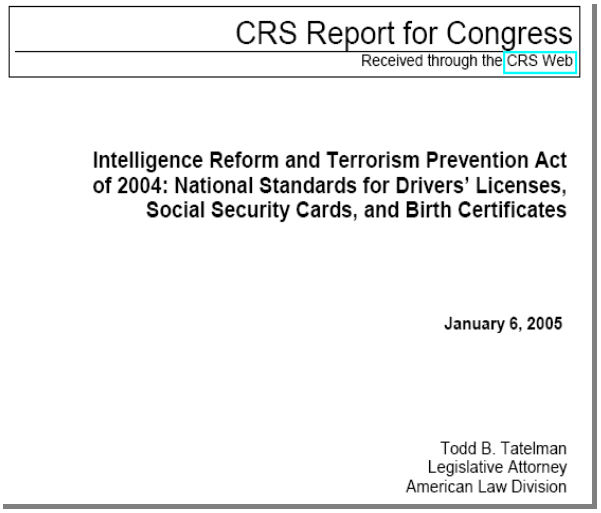
[67] Ver Glosario al final del material de estudio

para la que se necesitaban varios analistas de inteligencia durante días, con ASAP se puede llevar a cabo en una hora".

El reporte "*Byting Back: Regaining information superiority againts 21st Century insurgents*", presentado por la Rand Corporation al Departamento de Defensa de los EE.UU en el año 2007 acota que "precisamente lo que abre perspectivas inéditas al futuro de las guerras y especialmente del acopio de información y su uso para influir en las poblaciones de los países ocupados, es la presencia de estas nuevas tecnologías..."

EE.UU. ha desarrollado un grupo de acciones para "observar" permanentemente, dentro de instituciones establecidas, a los países y organizaciones que consideran sus enemigos. En ese sentido creó en 2006 el denominado Grupo de Tareas para la Libertad Global de la Red (*Global Internet Freedom Task Force – GIFTF*), una organización multi-agencias subordinada al Departamento de Estado, que se concentra fundamentalmente en China, Irán y Cuba.

De la misma manera, aprobó la "*Ley de Reforma de Inteligencia y Prevención del Terrorismo del 2004*", que entre otros objetivos tiene el de lograr que las 15 agencias de espionaje trabajaran bajo la égida del Director de Inteligencia Nacional, y considera entre las medidas la de "desarrollar herramientas informáticas potentes, capaces de acceder y procesar enormes cantidades de información sobre personas que resulten de interés para la comunidad de inteligencia", así como "potenciar el papel de los analistas, su preparación y cooperación entre los homólogos de las distintas agencias" y "crear comunidades virtuales de analistas que puedan intercambiar ideas y conocimientos con seguridad, así como utilizar tecnologías de punta para investigar, acceder, compartir información y criterios analíticos".



CRS Report for Congress

Received through the CRS Web

Intelligence Reform and Terrorism Prevention Act of 2004: National Standards for Drivers' Licenses, Social Security Cards, and Birth Certificates

January 6, 2005

Todd B. Tatelman
Legislative Attorney
American Law Division

Un aspecto explícito en dicha Ley es, además de crear una base de datos común, "utilizar dinámicamente los avances científico técnicos de punta, en esferas como las biociencias, nanotecnologías y la informática, asegurando el esfuerzo de I+D necesario para que las ideas se puedan convertir rápidamente en herramientas útiles y rentables para la comunidad de inteligencia".

Otros elementos relacionados con el control de la información, quizás más conocidos, son:

- Los proveedores de servicios de comunicaciones e Internet están obligados a dejar "puertas traseras" en sus diseños para la intersección de datos, voz y texto.

- Participan en este círculo las grandes corporaciones productoras de equipos, sistemas y aplicaciones, como Microsoft, IBM, Oracle, Intel, AMD, Yahoo, Cisco, Google, Apple, entre otras.

Merece mención aparte la red Echelon, que se considera la mayor red de espionaje y análisis para interceptar comunicaciones electrónicas de la historia. Controlada por la comunidad UKUSA (EE.UU., Canadá, Reino Unido, Australia y Nueva Zelanda), puede capturar comunicaciones por

radio y satélites, llamadas telefónicas, fax y correos electrónicos en casi todo el mundo e incluye análisis automático y clasificación de las interceptaciones. Se estima que Echelon intercepta más de mil millones de comunicaciones por hora. A pesar de haber sido presuntamente construida con el fin de controlar las comunicaciones militares y diplomáticas de la URSS y sus aliados, se ha utilizado para encontrar pistas sobre tramas terroristas, planes del narcotráfico e inteligencia política y diplomática. También ha sido usada para el espionaje económico y la invasión de privacidad en gran escala. La existencia de Echelon fue hecha pública en 1976.

En mayo de 2001, el Parlamento europeo emitió una declaración, donde expresaba que no había razones para dudar de la existencia de Echelon. Sin embargo, se considera que desde los primeros años de los 90 del pasado siglo, la Unión Europea creó la red Enfopol, como respuesta a Echelon.

Por otra parte, DARPA – Agencia de Proyectos de Investigación Avanzada de la Defensa, creada en 1958, enfocada a proyectos de corto plazo, la que cuenta entre sus logros con la red "Arpanet", la que evolucionó en el tiempo hacia la actual Internet como la conocemos, estableció en 2002 la *Information Awareness Office – IAO*, con el objetivo de unificar varios proyectos de las TIC vinculados con la seguridad nacional. Su misión fue la de "imaginar, desarrollar, aplicar, integrar, demostrar y utilizar las tecnologías de la información, componentes y otros sistemas de información para detectar amenazas asimétricas, con el objetivo de lograr un Conocimiento Total de la Información" (*Total Information Awareness – TIA*). Un consejero del entonces presidente Bush, Steven Wallace, declaró: "El complejo mecanismo de espionaje podrá asociar una foto de Malasia tomada por un satélite con una llamada realizada en Fráncfort y con un depósito bancario en Pakistán para luego seleccionar todos esos elementos con algo que pasará en las calles de Chicago". Este programa, que supuestamente culminó en 2003, renombrado como *Terrorism Information Awareness Program*, contaba con más de 16 proyectos, siendo el más abarcador de los programas informáticos conocidos hasta la fecha, orientados a identificar y obtener de forma masiva información de carácter personal, financiera y gubernamental, tanto de fuentes públicas como privadas a nivel internacional. Así, investigó, desarrolló e integró tecnologías para agregación virtual de datos, análisis de enlaces relacionados con determinados contenidos, desarrollo de modelos descriptivos y predictivos a partir de técnicas de minería de datos o hipótesis humanas y aplicación de esos modelos a juegos de datos para, supuestamente, identificar terroristas.

En este mismo sentido, los EE.UU. desarrollaron el sistema *Carnivore* para espiar por parte del FBI los correos electrónicos. Su existencia se conoció a partir de que en 2000 un proveedor de servicios de Internet se negó a instalarlo y la disputa generó protestas de grupos de libertades civiles de todo el mundo. Fue rebautizado como DCS-1000, descontinuado en 2005 y sustituido por el DCS-3000, que según la revista técnica *Wired*, es "la red más intrincada en la telecomunicación para monitorear a sospechosos". En octubre de 2006 una organización de abogados y defensores de los derechos civiles, la *Electronic Frontier Foundation*, denunció la existencia de este desarrollo, aunque no se le hizo caso. En nombre de la "guerra contra el terrorismo", el FBI se negó a entregar los documentos confidenciales sobre esta herramienta, a pesar de que estaría obligado a hacerlo de acuerdo con la Ley para la Libertad de Información.

Posteriormente, en 2007 se conoció que el Ministerio de Defensa español trabajaba en un "*Carnivore*" europeo mejorado.

Un paso mejorado en los sistemas inteligentes de espionaje lo constituye la Infraestructura de Inteligencia Semántica Operacional (conocida por sus siglas en inglés OSEMINTI), iniciativa liderada por Francia con la participación de España e Italia.

Otros hechos interesantes son como a partir del año 2007 se desata una campaña que dura hasta nuestros días, criminalizando a Rusia por los ciberataques que sufrió Estonia. También la R.P.China ha sido acusada por ataques o penetración de redes en Estados Unidos, Corea del Sur y otros países, y, por supuesto, los integrantes del "Eje de Mal" de W. Bush, se encuentran en la mira acusados sobre preparativos para la ciberguerra, la guerra asimétrica en el ciberespacio y otras denominaciones. En agosto de 2008 durante la invasión de Georgia a Osetia del Sur se produjeron ataques cibernéticos contra Georgia, de los que fue acusada Rusia.

A finales de 2009 se conoció sobre el proyecto INDECT, financiado por la Unión Europea con 11 millones de euros, en el que trabajan la policía norirlandesa e investigadores de universidades de diez países europeos. Este proyecto consiste en crear una infraestructura para el registro e intercambio de datos y contenido multimedia, así como su procesamiento inteligente para detectar automáticamente "amenazas, comportamientos anormales o violencia". Se nutriría principalmente de imágenes captadas por las cámaras de videovigilancia instaladas en espacios públicos, pero se comprobó que se proyectaba la construcción de agentes encargados de monitorear automáticamente páginas web, foros de discusión en la red, redes punto a punto e incluso computadoras personales.

Un ejemplo concreto de acciones de esta naturaleza, conocido internacionalmente y de forma masiva fue el reconocimiento público en 2007 de que el conocido sistema operativo Windows Vista fue desarrollado de conjunto por Microsoft y los servicios secretos de los EUA, aunque la compañía desarrolladora aseguró que la Agencia de Seguridad Nacional (NSA) "solamente" colaboró en el desarrollo de las medidas de seguridad contra ataques.

En todo este escenario, nuestro país, objeto del más brutal bloqueo conocido por la historia, ha tenido que enfrentarse además a dificultades específicas asociadas a la imposibilidad de descargar directamente desde Internet determinadas aplicaciones o acceder a repositorios de códigos de aplicaciones, imprescindibles para nuestro necesario desarrollo en estas tecnologías.

Cuba, con pocos recursos económicos y con una población escolarizada y capacitada para acceder a las TIC, asume la informatización asediada por EUA, símbolo del capitalismo mundial, creador y líder de tecnologías y contenidos en la red, con planes concretos y recursos para utilizar estas tecnologías para subvertir y derrocar a la Revolución; ejemplo reciente es el documento publicado en julio de 2010 en la red de redes por el denominado "Grupo de Estudios sobre Cuba", titulado "Apoyo al Pueblo Cubano a través de la Tecnología: Recomendaciones para Líderes del Sector Público y Privado"

V- La informatización de la sociedad cubana

> *A un plan obedece nuestro enemigo: de enconarnos, dispersarnos, dividirnos, ahogarnos. Por eso obedecemos nosotros a otro plan: enseñarnos en toda nuestra altura, apretarnos, juntarnos, burlarlo, hacer por fin a nuestra patria libre. Plan contra plan.*
>
> ***José Martí***

La ideología dominante en una sociedad se expresa a través de la vida cotidiana de sus ciudadanos y ésta, a su vez, es la vía para la reproducción de los valores hegemónicos en ella. En la sociedad capitalista, el desarrollo y expansión de las Tecnologías de la Información y las Comunicaciones (TIC) –junto a sus implicaciones económicas, tecnológicas, militares, educativas y de consumo cultural, entre muchas otras– es también la expresión en este nuevo espacio, a nivel global, de los valores dominantes en esa sociedad que, lejos de retroceder, encuentran aquí un nuevo espacio de reproducción y también de manifestación de las contradicciones que le son inherentes.

En ese escenario, el impacto real de las TIC está determinado por la posición ocupada en el mundo contemporáneo (medios económicos, desarrollo y costo del acceso, nivel de preparación, disponibilidad de tiempo en la sociedad más allá del empleado en la supervivencia…). Esto explica cómo sus alcances por amplios e inabarcables que sean, al igual que el de los medios de comunicación masiva –cada vez más condicionados por los llamados filtros constituidos por la propiedad, los anunciantes y las fuentes- son jerarquizados y promovidos en función de perpetuar la hegemonía cultural del capitalismo, sin obviar las correcciones represivas cuando algo se sale de los marcos admisibles por el sistema. Con la expansión de las TIC, el capitalismo expresa otra vez su capacidad de asimilar la innovación, la iniciativa individual, e incluso la contracultura, y utilizarlas para su propia legitimación como portador de "democracia, libertades y derechos".

Cuba, con un proyecto de desarrollo que tiene como pilares la justicia social, la participación popular, la equidad y la solidaridad, ha diseñado e iniciado la aplicación de estrategias que permiten convertir los conocimientos y las tecnologías de la información y las comunicaciones (TIC) en instrumentos a disposición del avance y las profundas transformaciones revolucionarias.

Se señala que a partir del rol que desempeñan las TIC, en nuestro país:

- La Informatización de la Sociedad es un **imperativo** del país para poder desarrollarnos en las condiciones del mundo actual.
- El proceso de Informatización va a influir paulatinamente y de manera creciente **en todos los aspectos** de la vida de las instituciones y los ciudadanos.
- La Informatización **requiere recursos financieros, humanos y materiales** que debemos tratar de ir cubriendo. Podemos hacer mucho organizando bien lo que tenemos hoy.
- Se requiere **potenciar el papel de los Gobiernos locales en función de aprovechar las capacidades de cada territorio**, en base a una estrategia de informatización diseñada a partir de sus particularidades.

La Resolución Económica del V Congreso del PCC dejó orientada la voluntad política para desarrollar el proceso de informatización y las disposiciones legales que la institucionalizan establecen el trabajo conjunto del MIC con los órganos de Gobierno, los demás OACE y los OLPP para lograrlo. En el contexto actual resulta conveniente evaluar la manera de organizar,

regular y trazar las líneas de desarrollo integral de las TIC en Cuba, lo que deberá conducir a un incremento en la productividad, la eficiencia, la calidad de las producciones, el ahorro de materias primas y de portadores energéticos, contribuyendo a la sustitución de importaciones y asegurando la calidad necesaria para las exportaciones en las ramas priorizadas o de mayor impacto en la economía nacional, así como hacer sostenible el aumento de la calidad de vida de los ciudadanos, tomando en cuenta el uso que la agresión imperialista pretende hacer de estas tecnologías.

Durante 1996 se trabajó en la coordinación de grupos de trabajo de los organismos más vinculados a la industria informática, con el objetivo de estudiar la situación nacional e internacional de la mencionada industria. Estos grupos, mediante un proceso de captación y análisis de información, estudio, discusión en grupo y conformación de conclusiones y proyecciones, elaboraron los documentos "***Diagnóstico del sector de actividad de la industria electrónica en Cuba***" y "***Estado actual y tendencias de la industria de la información***", que sirvieron de marco informativo y conceptual para la elaboración, en 1997, de los "***Lineamientos estratégicos para la informatización de la sociedad cubana***", los cuales fueron redactados por especialistas del entonces Ministerio de la Industria Sideromecánica y Electrónica, el Ministerio de Ciencia, Tecnología y Medio Ambiente, el Ministerio de Educación Superior, el Ministerio de Comunicaciones y el Ministerio de Justicia. En el proceso de captación y análisis de información se contó con el valioso apoyo de un diverso grupo de consultores de varios organismos, con los que eventualmente se discutieron aspectos cubiertos por el documento, de acuerdo con las áreas de trabajo de cada cual.

En ese documento se significaban los siguientes objetivos generales para el proceso de informatización:

1. Incrementar la eficiencia de la producción y los servicios para lograr aumentar su competitividad, mediante el aumento de su calidad y la disminución del consumo de recursos materiales y de portadores energéticos.
2. Aumentar la efectividad y facilitar la toma de decisiones en la gestión de dirección mediante la información, confiable y con la mayor actualización, a los órganos de gobierno y a la administración a todos los niveles, sirviendo de apoyo al desarrollo integral y multifacético de la sociedad cubana.
3. Generar una fuente de divisas mediante la exportación y la venta en frontera, proveniente de la industria informática y en especial mediante el incremento de la industria del software.
4. Elevar la calidad de los servicios públicos, en especial la educación, la salud y la seguridad social.
5. Mejorar los servicios que brinda el Poder Popular al disminuir el tiempo medio de atención a la población y minimizar los trámites que debe realizar el ciudadano
6. Brindar al mundo, mediante INTERNET y otras vías, información fidedigna sobre el proceso revolucionario cubano, su realidad política, social y económica, su desarrollo científico y cultural, las posibilidades económicas, de inversión y sus bondades turísticas.
7. Brindar a los profesionales, investigadores, educadores, estudiantes y funcionarios de las entidades la información científica, tecnológica y comercial actualizada existente en el mundo mediante un acceso a INTERNET y otras vías de intercambio de información en forma organizada y controlada.

En la actual coyuntura un reto se nos impone: nuestro país está obligado a desplegar y ejecutar una política de seguridad orientada a alcanzar, paulatinamente, la invulnerabilidad y la soberanía e independencia tecnológicas. **Este desafío adquiere una magnitud significativa, en tanto no debe frenar el desarrollo del proceso de Informatización**. Resulta imprescindible, por tanto, establecer mecanismos de identificación, evaluación, eliminación o reducción de riesgos, así como acciones de contingencia.

Nuestro proceso de informatización de la sociedad –seguro, ordenado y masivo– constituye desafío inevitable y oportunidad para la hegemonía socialista y antiimperialista en nuestro país. Es oportunidad para promover y potenciar los valores de solidaridad, culto al conocimiento y a la laboriosidad y para expresar y desarrollar la democracia socialista y la participación activa del pueblo como parte esencial de ella, creando condiciones para asumir exitosamente la lucha ideológica en que nos encontramos envueltos. El uso seguro, ordenado y masivo de las TIC debe contribuir a la soberanía nacional e independencia tecnológica y es herramienta de eficiencia, catalizadora del desarrollo sostenible. Como principio, el Estado cubano nunca ha conceptualizado las TIC como un fin en sí mismas, sino como una herramienta para el desarrollo de todas las esferas de la sociedad y actualmente se profundiza en su papel para lograr la seguridad y soberanía tecnológica de nuestro país. Son soporte para el desarrollo sostenible y la defensa de la Revolución Cubana

Los principios fundamentales del proceso de informatización son: la defensa política y técnica del país frente a las amenazas, los ataques y riesgos de todo tipo, apoyo a las prioridades del país, uso de las TIC y su acceso por los ciudadanos, el desarrollo de aplicaciones nacionales y la utilización preferente de código abierto, la modernización de la gestión y servicios del Gobierno, el Estado, el sistema empresarial y demás entidades y la ampliación de las tareas de Investigación-Desarrollo e Innovación (I+D+i).

Existen factores que influyen negativamente en la informatización: insuficientes ingresos por la industria de las aplicaciones informáticas, regulaciones económicas que no posibilitan su financiamiento y desarrollo; insuficiente percepción en directivos de la importancia de las TIC para la seguridad nacional y para el mejor desenvolvimiento de sus entidades; dificultades en la ubicación de los graduados en TIC, incremento de emigración de especialistas del sector, proliferación del desarrollo de aplicaciones sin control ni ingresos para la nación.

Algunos antecedentes.

En enero de 1997 se aprueba el documento "Lineamientos Generales para la Informatización de la Sociedad Cubana", con una vigencia de tres años. Concluido ese período, se constituyó el Ministerio de la Informática y las Comunicaciones (MIC)[(68)], aglutinando la acción estatal, dispersa hasta entonces en varios organismos, y dentro del mismo se creó la Dirección de Informatización de la Sociedad, cuya primera tarea fue revisar los lineamientos aprobados, concluyéndose que los mismos mantenían plena vigencia.

[68] El acuerdo 3736 del CECM (18-07-2000) asignó al MIC establecer, regular y controlar la política y las estrategias para el desarrollo, evolución, producción, comercialización y utilización de las TIC y sus servicios, la industria electrónica y la automatización, los servicios postales y el acceso a las redes de infocomunicaciones con alcance global.

En esa etapa, en el país se produce un crecimiento de equipamiento e infraestructura de conectividad, cuya coyuntura más significativa fue la decisión del Comandante en Jefe de llevar la computación a todas las escuelas del país, tarea cumplida en marzo de 2002 y que planteaba la necesidad de enfocar el desarrollo de la informatización con mayor dinamismo, a través de la formulación de Programas y Proyectos que permitieran concretar acciones.

A finales de 2002, el MIC propone crear la Oficina para la Informatización, lo que fue aprobado en marzo de 2003. En mayo del propio año, se decide llevar al Consejo de Ministros una propuesta concreta de proyectos de importancia nacional en los que se proponía trabajar con prioridad, la que resulta aprobada, acordándose su chequeo transcurrido un año.

En abril de 2004 se presenta al Consejo de Ministros la situación alcanzada en cada uno de los mencionados proyectos, con su correspondiente actualización. En esta sesión el Consejo tomó una serie de acuerdos específicos, para continuar el desarrollo del proceso de informatización cubano.

Tales acuerdos establecían que, el MIC y su oficina, asumían la responsabilidad de su ejecución. A la luz del tiempo trascurrido se pudo concluir que; al no ser el propio Ministerio ejecutor principal, esto trajo como consecuencia que los organismos implicados no siempre asumieron la responsabilidad en el cumplimiento de los acuerdos, constituyendo una deficiencia que se sumó al hecho de que ninguna otra disposición jurídica, salvo para la seguridad informática, fuera emitida por el MIC con respecto al proceso de informatización.

A partir de todo el proceso descrito, las áreas clave del proceso de informatización en nuestro país actualmente son:

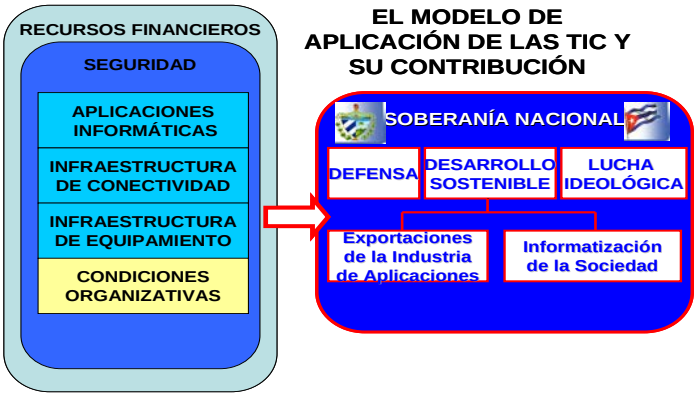
- desarrollo de las infraestructuras;
- garantizar la formación, tanto desde el punto de vista de la educación regular, la formación especializada, como la formación de toda la población;
- fomentar la industria nacional, en particular la de aplicaciones informáticas;
- impulsar proyectos de investigación, desarrollo e innovación tecnológica;
- impulsar la informatización en el campo de la toma de decisiones para la dirección;

Sobre estos elementos, lograr entonces salidas a manera de programa y proyectos en las áreas:

- informatización para el gobierno y la actividad empresarial;
- informatización para los ciudadanos.

Modelo de aplicación de las TIC y su contribución:

El modelo utilizado, aplicable al proceso en su conjunto y a cada programa o proyecto en particular, permite identificar elementos que, sin ser los únicos, se han agrupado de la siguiente manera (ver gráfica)



Donde:

- Condiciones organizativas: se considera la capa "básica". Se compone de la autoridad que conduce

el proceso, los expertos funcionales en la actividad de que se trate; el marco jurídico, regulatorio y metodológico; el desarrollo organizacional y la instrumentación de políticas tecnológicas, de conexión, de acceso y de utilización. Incluye los recursos humanos: plantilla, cuadros, especialistas y técnicos, formación y capacitación.

- Infraestructura en equipamiento: incluye tecnología, equipos y soluciones acordes a los requerimientos, redes locales, servicios técnicos, modernización, reciclaje y consumo energético.
- Infraestructura de conectividad: abarca tecnología, redes y equipos asociados al transporte de datos, protocolos y estándares, conexiones remotas, utilización de centros de datos remotos.
- Aplicaciones y Servicios Informáticos: compuesta por la especificación de necesidades, utilización de estándares, diseño de los servicios requeridos, identificación de disponibilidades, implementación, desarrollo y soporte técnico a la explotación. Sistemas operativos, herramientas y utilitarios, aplicaciones. En esta capa tiene un importante papel la Migración hacia estándares abiertos.
- El sistema de seguridad, que abarca todas las partes componentes, ha sido insuficiente hasta el momento. Su diseño, en los casos donde ha existido, no se ha estructurado de manera coherente y sistémica. Es el área hacia donde se dirigen los mayores esfuerzos del Ministerio de la Informática y las Comunicaciones.

Todo el modelo está condicionado por la capacidad disponible de Recursos Financieros: fuentes, inversiones, costos de operación y de sostenibilidad técnica (partes y piezas, reparaciones y mantenimiento), así como los insumos. En dependencia de la disponibilidad de los recursos financieros, se adapta el programa o proyecto en varias etapas de ejecución. Por ello, en el Plan de cada institución receptora de productos y servicios vinculados con programas y proyectos priorizados, deberá inscribirse una partida presupuestaria para la informatización de su sector, en dependencia de lo que previamente se haya pactado con las empresas suministradoras.

Las prioridades del país determinan cuáles Programas y Proyectos respaldar con recursos: enfrentamiento a la ciberagresión imperialista; informatización del Gobierno; la dirección por objetivos y los sistemas de información; la gestión integrada; la producción agroalimentaria; el ahorro energético y el fondo habitacional; la voluntad hidráulica y la automatización de procesos.

Incluye el desarrollo de la industria de aplicaciones informáticas y la informatización de los servicios sociales básicos, sustentado todo en la importancia que se le debe prestar desde cada institución.

Principales programas y proyectos:

Como plataformas fundamentales para el despliegue de los diferentes Programas y Proyectos contenidos en el Proceso de Informatización de la Sociedad, se han definido dos programas de singular importancia. Estos son:

- **Programa "Red Cuba":** Dirigido a la integración ordenada de las redes, mediante soluciones informáticas integrales y proyectos que proporcionan coherencia. Permite el acceso de la sociedad a la información y a los servicios públicos.

Entre los proyectos que integran este programa, vale señalar:

- **Proyecto de Soluciones informáticas:** Las opciones de disponibilidad de Soluciones Informáticas a partir de adquisición de partes y piezas, del reacondicionamiento de equipos ya en uso y otras propuestas. Abarca los siguientes aspectos:

  - ❖ soluciones informáticas en estaciones de trabajo: terminales PC sin disco, importadas; servidores para PC sin disco importados; terminales de PC sin disco, obtenidas de reacondicionamiento industrial y terminales de cliente ligero importadas, entre otras.
  - ❖ soluciones informáticas de conectividad
  - ❖ soluciones informáticas en nodos: agrupamiento (*clúster*) de procesamiento y de almacenamiento, equivalentes a servidores de bajas, medias y altas prestaciones, con identificación de su equivalencia ("servidores optimizados", a partir del reacondicionamiento por la industria electrónica nacional.
  - ❖ soluciones en sistemas y aplicaciones informáticas

- **Proyecto de Infraestructura de Clave Pública (PKI):** Permite otorgar certificados digitales y firmar digitalmente documentos. La infraestructura deberá basarse en estándares, ser flexible y adaptativa, así como garantizar una seguridad razonablemente efectiva.

- **Proyecto de Arquitectura, Normas y Estándares**: definido para lograr la interoperabilidad entre los diferentes sistemas que se utilizan en las soluciones al gobierno y la administración central del Estado, en su primera fase. Abarca los componentes relacionados con la presentación de la información, el procesamiento y el almacenamiento de los datos.

- **Proyecto Buscador y Portal "2x3"**. Publicados desde la Oficina para la Informatización. http://www.2x3.cu

  El **Portal**, dirigido al ciudadano cubano, consta de varios canales, entre los cuales, el de trámites de la población, respaldado por el grupo de trámites de la Asamblea Nacional del Poder Popular, tiene información sobre 182 trámites y 134 servicios.

  El **buscador** permite realizar búsquedas en miles de páginas cubanas. Incorpora un directorio de sitios según temáticas.

  Como parte de los servicios en línea de facilitación social que se desarrollan, funciona, desde el mes de septiembre de 2009, la **Bolsa de Permutas**, http://www.permutasencuba.cu la cual se realizó en colaboración con el Instituto Nacional de la Vivienda (INV). Además de tener acceso a una amplia base de datos de permutas, es posible consultar documentos legales relacionados con la vivienda.

- **Enciclopedia Colaborativa Cubana, EcuRed,** http://www.ecured.cu. Proyecto para construir colectivamente el conocimiento, en primer lugar de los cubanos, nuestro saber, difundirlo y compartirlo con el mundo de habla hispana. Busca concentrar y desarrollar el conocimiento desarrollado por las instituciones y especialistas cubanos, de manera que se conviertan en sus líderes y lo conduzcan desde su capacidad intelectual y profesional como garantía de su rigor y calidad.

- **Proyecto Bases de Datos del Ciudadano y de Direcciones.** Indispensable para el fortalecimiento de los procesos que involucren al ciudadano y la reducción de errores e

ilegalidades.

- **Proyecto plataforma de cobros y pagos en línea.** Encaminado a contar con una plataforma que permita ejecutar los pagos y cobros en línea.

- **Programa "Estándares Abiertos".** Como parte de las acciones encaminadas al fortalecimiento de los niveles de seguridad, invulnerabilidad e independencia tecnológica de nuestros sistemas informáticos, se trabaja en la sustitución ordenada de todas aquellas aplicaciones sobre plataformas propietarias, por otras de código abierto, cuya evaluación previa haya demostrado estabilidad, seguridad, interoperabilidad, así como su factibilidad de ser auditadas.

  Iniciado pilotaje de migración en los organismos: IACC, MIC, MINSAP, MINED, MES y MINCULT.

  Un programa en sí mismo, el de "Desarrollo, Implementación y Sostenibilidad de un Sistema Integrado de Gestión" (SIG) – CEDRUX, se está desarrollando totalmente sobre plataformas abiertas, y se ha probado sobre soluciones informáticas nacionales (distribución cubana de sistema operativo y aplicaciones en código abierto – NOVA, y equipamiento de tipo terminales de PC sin discos duros).

Otros programas contenidos en el Proceso Nacional de Informatización de la Sociedad, que se soportan sobre los dos anteriores, son:

- **Programa "Desarrollo, Implementación y Sostenibilidad de un Sistema Integrado de Gestión" (SIG) – CEDRUX:** Este Programa persigue el desarrollo en el país de Sistemas Informáticos al estilo de los Sistemas de Planeamiento de Recursos Empresariales (*Enterprise Resource Planning – ERP*) para cubrir, primeramente, los módulos del área contable – financiera, y a corto y mediano plazo, el resto de los módulos de las diferentes áreas a gestionar tanto en Organismos y Órganos del Gobierno y el Estado, como en las instituciones a ellos vinculadas.

- **Programa "Informatización de Sectores Sociales":** Dirigido a la informatización de la Salud, la Educación, la Cultura y a los Joven Club. Entre los proyectos que integran este programa están:

  - **Proyecto "Informatización de la Salud Pública"**
  - **Proyecto "Informatización de la Educación: Enseñanza General".**
  - **Proyecto "Informatización de la Educación: Enseñanza Superior".**
  - **Proyecto "Informatización de los Joven Club de Computación y Electrónica"**

- **Programa "Informatización del Gobierno":** Programa que se elabora a partir de la modernización del anterior "Gobierno en Línea" que estaba encaminado a la informatización de la gestión del Sistema del Poder Popular. Este programa está en proceso de reelaboración, a partir del reordenamiento del Estado. Se avanza en estos momentos en el desarrollo de la Red Propia de Datos del Gobierno en todos los Consejos de la Administración Provinciales y Municipales (CAP y CAM), el Comité Ejecutivo del Consejo de Ministros (CECM) y los nodos centrales de los OACE y otros organismos, como primera fase de despliegue, además de valorarse y desarrollarse diferentes aplicaciones informáticas para su utilización.

- **Programa "Ciudadano":** Programa encaminado a desarrollar diversos proyectos con el objetivo de brindar informaciones de trámites y servicios a la población mediante el uso de

las TIC. Entre los proyectos que integran este programa destacan:

- **Proyecto Trámites de Vivienda:** Proyecto para la creación de la infraestructura necesaria que permita garantizar la gestión administrativa del Sistema de la Vivienda y brindar los servicios de trámites a la población mediante el uso de las TIC.
- **Proyecto Oficina de Cobros de Multas:** Persigue la informatización del proceso del Cobro en las Oficinas de Multas.
- **Proyecto Trámites de la OFICODA:** Persigue la informatización de los trámites de las Oficinas de Registro de Consumidores, OFICODA.

➢ **Programa "Puerto – Transporte - Economía Interna:"**

Este programa pretende enlazar coherentemente la información de los diferentes eslabones de la cadena Puerto-Transporte-Economía Interna, a los efectos de una mejor toma de decisiones alrededor de los procesos vinculados con la misma.

Entre los proyectos integrantes del programa señalan:

- **Proyecto "Sistema Único de Aduanas":** desarrollado prácticamente todo sobre plataformas de código abierto, y referencia nacional de la utilización de estas tecnologías, abarca en un sistema interoperable diferentes componentes que permite la interacción de las diferentes instituciones y procesos que transcurren en el sistema aduanal.
- **Control de Flotas:** Permite el control y gestión de las flotas de transporte, utilizando parte de la incipiente Infraestructura de Datos Espaciales de la República de Cuba (IDERC), la cual a su vez constituye otro programa de informatización.
- **Proyecto "Informatización de la Unión Nacional de Alimentos" (UNAL):** Proyecto para la creación de la infraestructura tecnológica necesaria que permita garantizar la toma de decisiones y la gestión eficiente de los almacenes, unidades básicas y estructuras transportistas que conforman la Unión Nacional de Alimentos.

➢ **Programa "Infraestructura de Datos Espaciales de la República de Cuba" (IDERC):** Programa para el desarrollo de los mapas digitales a las escalas necesarias que permitan el desarrollo de sistemas de información geográficos (SIG) para la toma de decisiones, así como de diversos servicios de consultas geoespaciales, Está en línea el Portal Geoespacial con variada información y servicios temáticos.

➢ **Programa Comercio Electrónico:** Encaminado a impulsar el comercio electrónico; actualmente se reevalúa su alcance, aunque diversas instituciones realizan algunas actividades utilizando esta modalidad.

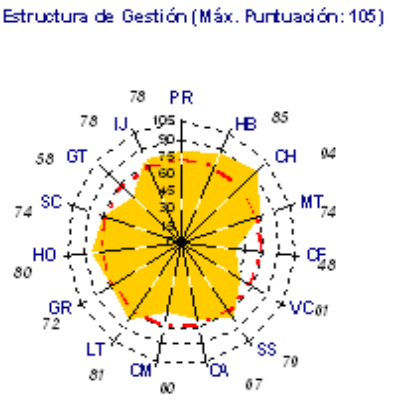
➢ **Programa "Agroalimentario":** El Programa "Incremento de la productividad y eficiencia en el sector agroalimentario mediante el uso de las TIC" está encaminado a incrementar la productividad y eficacia de la gestión de ese sector, contribuir a la eficiencia y competitividad del país y elevar la calidad de vida del pueblo.

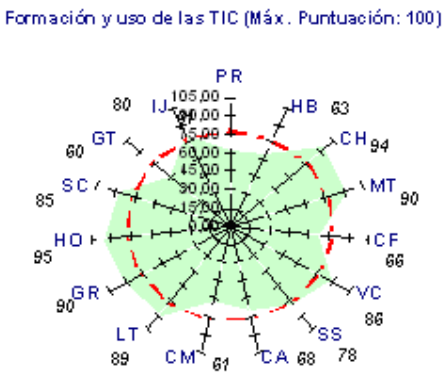
➢ **Programa "Informatización Industrial:"** Enfocado al incremento de la productividad y eficacia de la gestión de ese sector, contribuyendo a la eficiencia y competitividad del país y la elevación de la calidad de vida del pueblo. En proceso de elaboración de conjunto con el MINIL. Este Programa incluirá las características de los procesos industriales de otros OACE del sector, los que deberán incorporarse al programa.

Métrica nacional:

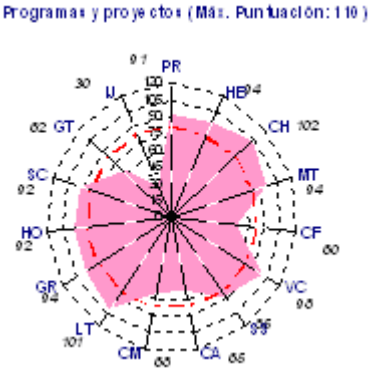
El Observatorio de las TIC en nuestro país, que radica en la Oficina para la Informatización, ha estructurado una métrica que se revisa sistemáticamente, compuesta por 4 grupos de indicadores que permiten conocer cual es la media nacional en cada uno de los aspectos que los grupos engloban así como en su conjunto. Estos indicadores, tanto aplicables a instituciones como a territorios, se ejemplifican a continuación (ajustados al caso territorios)

- Estructura de Gestión.- Incluye: funcionamiento del Grupo Provincial de Informatización y los municipales; existencia de Estrategia de Informatización provincial y municipales; presupuesto destinado a la Informatización; completamiento de los departamentos TI o equivalentes; análisis de los temas TI en los Consejos de la Administración y los resultados en los Controles Gubernamentales en estos temas.

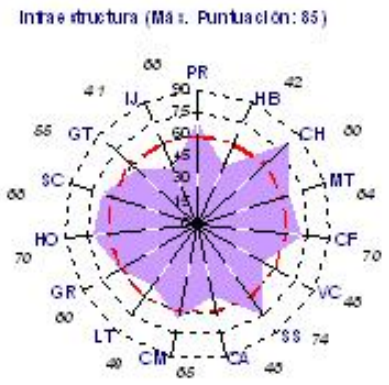




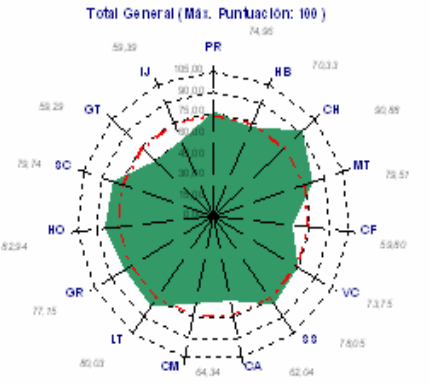
- Formación y Uso de las TIC.- Incluye: Graduados JCCE; eventos locales TIC; uso de las TIC por directivos del 1er nivel; participación y apoyo de directivos en eventos TIC; aptitudes del personal TIC en los Departamentos de TI o equivalentes.



- Programas y Proyectos.- Incluye: estado de los Programas y Proyectos Nacionales en las Provincias (Control y Gestión de Flotas, Bibliotecas Municipales, Salud, Joven Club, etc) y el estado de programas locales.



- Infraestructura.- Incluye: % PC en Redes Locales; Intranet; sitios WEB en los CAP-CAM; cobertura de aplicaciones informáticas en los Gobiernos; factibilidad para la formación en TIC (IPI, Universidades con carreras afines a las TIC, JCCE); acceso a las TIC (Pc x 100 hab.; cantidad de cajeros automáticos; centros de acceso público a servicios de correo electrónico e Internet x 10 000 hab.); otros datos obtenidos por encuestas o censos de la ONE.



Sobre la industria nacional de aplicaciones informáticas:

La exportación de servicios y productos de las TIC debe convertirse en importante fuente de divisas. El mercado se expande modestamente a otros países; surgen proyectos al margen del Convenio Cuba-Venezuela; la proyección hacia el resto del ALBA está por desarrollar.
Se estudia el rediseño de esta industria con un enfoque novedoso que posibilite una mayor productividad y mayores resultados en su gestión.
Las soluciones informáticas hacia lo interno son estratégicas por su efecto en el desarrollo económico y social. Están vigentes disposiciones por las que muchos de los servicios y productos que las empresas ofrecen están subsidiados, con lo cual no pueden cubrir sus costos y gastos con sus ingresos en ambas monedas. Se impone la revisión de esta problemática.

Algunos datos sobre la informatización de Cuba al finalizar el año 2010
Cantidad de computadoras: 724 000, de ellas, en las viviendas: 100 000
Usuarios de servicios de Internet: 1 790 000, de ellos, navegación plena: 454 000
Páginas cubanas en la red: más de 500 000
Digitalización de la telefonía: 97,43%
Abonados a celulares: 1 003 015
Cantidad de redes propias de datos de instituciones: más de 20
Ancho de banda nacional promedio: 4 Mbps
Ancho de banda internacional: subida 189 Mbps bajada 393 Mbps

VI- Internet y la ciberguerra

> *La Red de Redes, que nació en un laboratorio del Pentágono, se ha convertido en la gran encrucijada de la sociedad actual. La capacidad tecnológica, la infraestructura, el acceso al conocimiento y recursos humanos calificados son fuentes decisivas de la competitividad y expresión en el mundo actual.*

Como la fuerza de gravedad, como la energía atómica, la Internet[69] no es ni buena ni mala. Fraternidad o egoísmo, audacia o retardo, eficacia o incompetencia son atributos de quienes emplean esta herramienta que, como el cuchillo, puede ser utilizada para facilitar el alimento –cultural o materialmente hablando–, como arma de defensa y, también, para amenazar y exterminar al prójimo a través de la muerte física –un misil teledirigido con precisión matemática– o digital –la exclusión de la sociedad en red–.

El nacimiento de la Red de redes en un laboratorio futurista del Pentágono ha generado justificados recelos. ARPANET, fuente principal de lo que acabaría siendo la Internet, fue ideada, diseñada y posteriormente gestionada por un grupo de militares y académicos al servicio de una de las instituciones más innovadoras del mundo, DARPA (Defense Advanced Research Projects Agency)[70], del Departamento de Defensa de los Estados Unidos. Sin el Pentágono, jamás estos especialistas habrían sido capaces de sumar por sí mismos los recursos necesarios para construir una red de computación que fusionara la infraestructura de redes ya existente a principios de la década del 60 y los sistemas de telecomunicaciones. El impulso político fundamental de la investigación no fueron las ideas libertarias o el altruismo científico de los brillantes informáticos de algunas de las más prestigiosas universidades norteamericanas que participaron en el proyecto, sino la Guerra Fría.

Para proveer una red de información segura y descentralizada que impidiera al "enemigo" destruir de una vez todo el sistema de información del Ejército norteamericano, investigadores universitarios, fundamentalmente de centros de altos de estudios en California, y los militares de la Agencia de Proyectos de Investigación Avanzada (ARPA, Advanced Research Projects Agency) cerraron filas para dotar a los halcones de la guerra de una herramienta poderosísima para el avance estratégico de la doctrina militar norteamericana.

Como ha explicado el teórico catalán Manuel Castells, coincidieron circunstancias únicas para el nacimiento de un medio que llegaría a convertirse en la base tecnológica que soporta a un tipo específico de sociedad humana: la sociedad en red. En un escenario ideal para que el Departamento de Defensa encabezara el desarrollo científico, la Guerra Fría, se articularon de un modo único la estrategia militar, la cooperación de grandes proyectos científicos, un determinado espíritu empresarial-tecnológico y la innovación contracultural[71].

---

[69] Internet es un protocolo de comunicación (TCP-IP) que permite a computadoras establecer una relación entre sí. "La Internet" es una red que permite a personas comunicar e informarse mediante el uso de máquinas y protocolos técnicos. Preferimos utilizar la expresión "la Internet", la cual se refiere a la interacción de la red humana y la red tecnológica, pero con los seres humanos en una posición jerárquica superior. La Real Academia de la Lengua no aclara el uso de esta palabra en masculino o femenino.

[70] Sería conocida como ARPA durante la Guerra Fría.

[71] Castells, Manuel: *La era de la información*. Alianza Editorial, Barcelona (tercera edición), 2005. Volumen 1: La sociedad en red, p.77

Fue determinante la doctrina de la superioridad técnica. Vinculada al militarismo, se consolidó en el pensamiento político norteamericano desde fines de los años 40, cuando se arraigó una forma de percepción social hegemónica en los Estados Unidos que se convirtió en el prisma a través del cual fueron interpretados desde entonces los acontecimientos globales y la puesta en práctica de la política estadounidense. El keynesianismo[72] militar apostó en primer lugar a superarmas de guerra que lograran intimidar y dominar a la URSS. Con la participación de los Departamentos de Estado y de Defensa, EEUU emprendió una serie de estudios secretos de alto nivel para determinar cuál debería ser la postura militar estadounidense frente las contingencias que eran vistas con gran alarma por el Presidente Harry Truman y la elite política bipartidista.

Bajo el membrete de Consejo de Seguridad Nacional-68 (NSC-68) nació gradualmente la carta magna de la era de la Guerra Fría. De carácter secreto hasta su publicación en 1975, pero ampliamente conocido por sus conclusiones, el NSC-68 esgrimió el entonces inédito argumento de que la economía de EEUU tenía una capacidad excedentaria y que altos niveles de gasto militar de manera permanente operarían como un estimulante de la economía, generando efectos multiplicadores sobre el empleo y el gasto, que permitiría absorber a los desempleados y las capacidades de producción ociosas de la industria estadounidense.[73]

El núcleo duro del Estado de Seguridad Nacional estaba allí y el NSC-68 proporcionó la estructura ideológica y teórica para impulsar el "Triángulo de Hierro"[74] militar-industrial que ha combinado desde entonces en los Estados Unidos los intereses de las industrias de manufactura y alta tecnología, el aparato político del Estado y el liderazgo civil del Pentágono y de los militares profesionales. Sólo raras veces el Triángulo de Hierro no ha sido completamente exitoso en su interminable búsqueda de niveles siempre mayores de gasto militar: al término de la Guerra de Vietnam y brevemente en los años 90 cuando la desaparición de la Unión Soviética condujo a un cierto nivel de confusión con respecto al rol y cuantía del gasto militar en la sociedad, ocasionando un serio declive del mismo.

De acuerdo con el investigador Richard Rhodes[75], el principal estímulo para aplicar el keynesianismo militar fue la "exageración de la capacidad de la URSS para imponer objetivos de expansión militar". El mito de la marea humana del Ejército Rojo amenazando Europa, que durante los cuarenta años de Guerra Fría serviría de coartada y acicate para el rearme de Estados

---

[72] Keynesianismo, teoría económica basada en las ideas de John Maynard Keynes, tal y como plasmó en su libro *Teoría general sobre el empleo el interés y el dinero*, publicado en 1936 como respuesta a la Gran Depresión en los años 1930. El keynesianismo militar es una política económica por la cual el gobierno destina grandes cantidades de gasto público en el ejército o el área de Defensa militar en general, en un esfuerzo para incentivar el crecimiento económico vía gasto público, siendo una variación específica y particular del keynesianismo. Ejemplos típicos de este tipo de políticas son la Alemania de los años 30, y la de los Estados Unidos durante y después de la Segunda Guerra Mundial (durante las presidencias de Roosevelt y Truman) y en la década del 80, con Reagan.

[73] Fred Block: "Economic Instability and Military Strength: The Paradoxes of the 1950. Rearmament Decision" *Politics and Society, 1980.* pp. 35-58.

[74] James M. Cypher llama "Triángulo de Hierro" a la conjunción del *establishment* militar, las agencias "civiles" que materializan la política militar norteamericana y las empresas privadas que se benefician de los contratos militares. Ver: Cypher, James M.: "El retorno del Triángulo de Hierro, la nueva propuesta militar" Dollars and Sense, revista bimensual sobre problemas económicos y de opinión, febrero 2002. Reproducido en http://www.iade.org.ar/iade/

[75] Rhodes, Richard: *Arsenals of Folly: The Making of the Nuclear Arms Race*. Alfred A. Knopf, Nueva York, 2007. Primera edición, pp.102-117.

Unidos y de la OTAN, respondía cabalmente a los requisitos de la amenaza exterior que habían perfilado los estrategas militares de Truman.

La imagen de la oposición irreconciliable entre las dos potencias alcanzaría su máxima simplificación de la mano de Paul Nitze, jefe de la Oficina de Planificación Política del Departamento de Estado y el principal redactor del NSC-68, preparado entre febrero y abril de 1950. "Nitze, de acuerdo a un estudioso del informe que se entrevistó con él sobre el tema, 'quería sacrificar una cierta racionalidad en el análisis de NSC-68**, al exagerar la amenaza (de la Unión Soviética) con la esperanza de que la reacción de los líderes de opinión estaría acorde con la amenaza."**[76]

La estrategia de satisfacer primero las necesidades para la defensa lógicamente puso en guardia a la Unión Soviética, que también siguió esta pauta, con la importante diferencia de que la economía de los EE.UU. amortiguaba mucho mejor que la soviética el impacto del aumento del presupuesto para los militares desviados de los ingresos federales.

En su libro de 1970, *Pentagon Capitalism: The Political Economy of War*, el ingeniero industrial Seymour Melman[77] afirma que "desde 1946 a 1969, el gobierno de EE.UU. gastó más de 1.000.000 de millones de dólares en las fuerzas armadas, más de la mitad bajo los gobiernos de Kennedy y Johnson – el período durante el cual la administración estatal [dominada por el Pentágono] fue establecida como una institución formal."

La tesis del libro de Melman se puede resumir brevemente. Existe dentro del sistema económico capitalista de los Estados Unidos una segunda política económica –el Complejo industrial Militar[78]-, técnicamente subordinada a la entidad mayor, que es el núcleo rector del sistema industrial primario, y el silencioso maestro de ámbitos cruciales de su vida política. Cada año la dirección de este estado interior, apelando a una mezcla de miedo y patriotismo, renueva su control sobre la porción más rica de los recursos de la nación, que luego desembolsa a sus sátrapas industriales.

A propósito de un análisis de esta obra de Melman, Thomas Woods, escribió: "Según el Departamento de Defensa de EE.UU., durante las cuatro décadas de 1947 a 1987 se utilizaron 7,62 millones de millones de dólares en recursos de capital. En 1985, el Departamento de Comercio estimó el valor de la maquinaria y equipamiento de la nación, y de la infraestructura, en 7,29 millones de millones de dólares. En otras palabras, la cantidad gastada durante ese

[76] Ibídem, p.104 (el subrayado es nuestro).

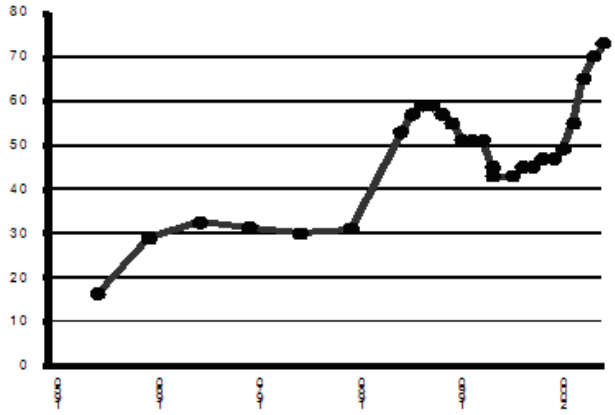
[77] Melman, Seymour: *Pentagon Capitalism: The Political Economy of War*. New York: Mc- Graw-Hill Book Company, 1970, pp. 2-3.

[78] En su último discurso como Presidente de los Estados Unidos, el 17 de enero de 1961, Dwight D. Eisenhower dijo: "*This conjunction of an immense military establishment and a large arms industry is new in the American experience. The total influence – economic, political, even spiritual – is felt in every city, every Statehouse, every office of the Federal government. We recognize the imperative need for this development. Yet we must not fail to comprehend its grave implications. Our toil, resources and livelihood are all involved; so is the very structure of our society.// In the councils of government, we must guard against the acquisition of unwarranted influence, whether sought or unsought, by* ***the military-industrial complex****. The potential for the disastrous rise of misplaced power exists and will persist.*"

período podría haber duplicado el capital social estadounidense o modernizado y reemplazado su inventario existente."[79]

Esta tendencia se ha mantenido inalterable hasta hoy, con otra tendencia hasta ahora irreversible: las inversiones en Investigación y Desarrollo (I+D) aumentan invariablemente de año en año. El Departamento de Defensa las destina a universidades y compañías privadas que trabajan a la carta proyectos militares, fundamentalmente en el ámbito de las tecnologías de la información y la nanotecnología, como indican los gráficos siguientes:

Inversión en I+D del Departamento de Defensa (1950-2000), en miles de millones de dólares:



Algunos de los principales programas de I+D del Departamento de Defensa, y las diez universidades y empresas que reciben mayores financiamientos del Departamento de Defensa, para desarrollar estos proyectos:

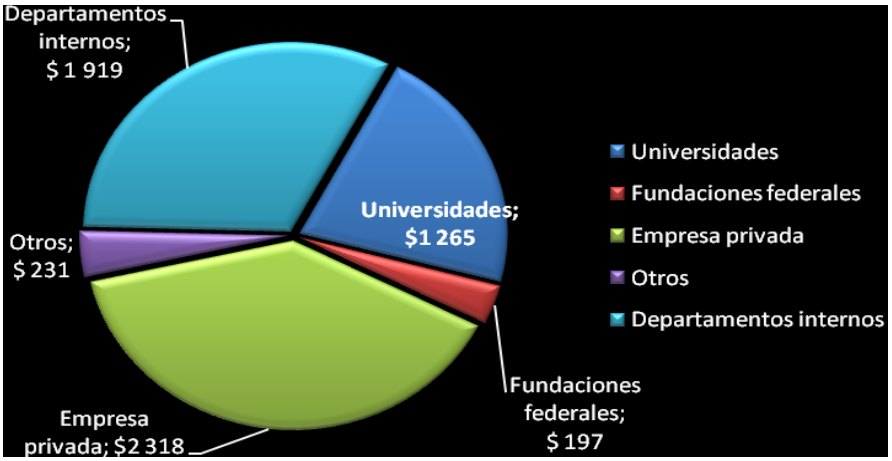
Partida	Presupuesto 2005 (MM $)
Defensa antimisiles	8 783
Avión de caza conjunto	4 326
Modernización de vehículos y otros sistemas blindados	2 268
Ingeniería de sistemas del "barco total"	1 164
Satélites de comunicaciones militares	607

Universidad	MM $ (2001)
John Hopkins University	341
Penn. State University	102
University of Texas Austin	85
University of Southern California	65
Georgia Institute of Technology	60
MIT	57
University of Washington	35
University of California LA	34
University of Southern Florida	34
University of Michigan	33

Empresa	MM $ (2002)
Lockheed-Martin	5 330
Boeing	4 310
Northrop Grumman	1 400
United Technologies	1 230
Raytheon	1 030
Boeing Sikorsky Comanche Team	660
General Dinamics	600
TRW	540
Sciencie Applications Int.	480
The Aerospace Corp	470

[79] Woods, Thomas: "The Neglected Costs of the Warfare State: An Austrian Tribute to Seymour Melman". Mises Institute, p.6. Puede consultarse en: http://mises.org/journals/scholar/woods2.pdf

Los enormes contratos militares y las iniciativas tecnológicas del Departamento de Defensa condicionaron no solo el tipo de sociedad que se perfilaría en el futuro –la sociedad en red–[80], sino el papel protagónico del Estado en esta transformación: "el Estado, no el empresario innovador en su garaje, tanto en los Estados Unidos como en el resto del mundo, fue el iniciador de la revolución de la tecnología de la información". Y tanto es así que la principal fuente de descubrimientos electrónicos, los Laboratorios Bell, desempeñaron en la práctica el papel de un laboratorio nacional subordinado al Pentágono, su principal contribuyente. La compañía matriz de Bell, ATT, disfrutó de un monopolio en las comunicaciones establecido por el gobierno, una parte significativa de sus fondos de investigación provino de este, rasgo que se ha mantenido en la actualidad, como se aprecia en el gráfico siguiente, que refleja el presupuesto para I+D del Departamento de Defensa en el año fiscal 2006 (en millones de dólares):



La propuesta federal de la cartera de I+D para el año fiscal 2009 es una cifra récord valorada en 147,4 mil millones de dólares, $ 4,9 mil millones más o un 3,5 por ciento este año por encima del actual nivel de financiación. El Departamento de Defensa tiene asignados 85,4 mil millones de dólares, un 6 por ciento más que en el 2008, a causa de un gran aumento para el desarrollo de armas espaciales para la NASA y para el apoyo de proyectos como el reactor termonuclear experimental internacional (ITER).[81]

Si durante el primer mandato del presidente Clinton, el gasto en I+D militar se intentó reorientar hacia las tecnologías de "doble uso" a fin de "potenciar la competitividad industrial de los EE. UU.", la Administración Bush ha abandonado esta política: ahora son las "necesidades" de la defensa las que orientan el gasto en I+D militar, y no la búsqueda de objetivos industriales ni de competitividad. El objetivo declarado es llevar a cabo la llamada "transformación" militar; una reorganización sustancial del ejército encaminada a conseguir, a través de la tecnología, la superioridad mundial en todo el espectro de las operaciones militares (desde los "conflictos de baja intensidad" hasta las "guerras con gran teatro de operaciones"). En consecuencia, los grandes –y prácticamente únicos- beneficiarios del incremento presupuestario han sido los programas de desarrollo de nuevos armamentos. Entre las nuevas armas, el mayor esfuerzo inversor de los EE. UU. se centra en el desarrollo del sistema de defensa contra mísiles balísticos

[80] Castells: La revolución de la tecnología de la información. T.1, p101.
[81] R&D Budget and Policy Program. American Association for the Advancement of Science, 2009. (En: http://www.aaas.org/)

(el polémico "escudo antimísiles") y en los armamentos de tipo ofensivo (aviones de combate, buques anfibios, modernización de tanques,...); con una especial prioridad a las armas no tripuladas, y a todo tipo de artilugios que permiten atacar objetivos a distancia: mísiles, proyectiles guiados, destructores y submarinos capaces de cargarlos, aviones espía no tripulados... Estas armas ofensivas o relacionadas con el "escudo", herederas del desarrollo de la red de telecomunicaciones y la microelectrónica, constituyen la mayoría de los 79 programas principales de armamentos del Pentágono, cada uno de los cuales supone una inversión mínima de 365 millones de dólares en I+D.

Como fruto de esta decidida apuesta por la I+D con fines armamentísticos, los EE. UU. Continuarán dominando en el futuro el desarrollo de la tecnología militar. Su determinación para adquirir nuevas capacidades -como la defensa antimisiles- asegura que la distancia respecto a otros países, tanto aliados como hostiles, sea cada vez mayor; creando así más dependencia en los primeros y aumentando la inseguridad y desconfianza en las relaciones con los segundos. La I+D militar es, además, un factor determinante a la hora de explicar por qué el gasto militar total de los EE. UU. es muy superior al de otros países. El presupuesto de Defensa estadounidense es unas 25 veces mayor que el gasto conjunto de los países identificados por el Pentágono como sus peores adversarios: Cuba, Irán, Libia, Corea del Norte, Sudán y Siria. Estos seis "enemigos", más Rusia y China, gastan en sus ejércitos menos de una tercera parte del presupuesto militar estadounidense. En cuanto a Iraq, en el momento de la invasión, su presupuesto militar era 285 veces inferior al de los EE. UU.

La dinámica pro-guerra se ve reforzada por la elevada "permeabilidad" existente entre la Administración de los EEUU y las industrias de armamento, con frecuentes tránsitos de cargos de una a otra. Por ejemplo, Lynne Cheney, esposa del vicepresidente Dick Cheney, estuvo en nómina de la Lockheed

Martin, primer proveedor de armas al Pentágono; y Donald Rumsfeld, ex secretario de defensa, dirigió una empresa aeronáutica que fue comprada por General Dynamics y presidió la General Instrument Corporation, dedicada a las tecnologías de transmisión de banda ancha, distribución y control de acceso a edificios. Michael W. Wynne, subsecretario de Defensa para adquisiciones, Tecnología y Logística y máximo responsable tanto de la I+D como de las compras del Pentágono, fue presidente de la división de espacial de la Lockheed Martin y trabajó en las divisiones de Aviones de Combate y Tanques de la General Dynamics, empresa de la que fue vicepresidente hasta 1999; mientras que Anthony Tether, director de la DARPA desde 1981, ha ocupado, entre otros, los cargos de Vicepresidente de la Corporación Aeroespacial Ford o CEO[82] de la compañía Dynamics Technology, notablemente comprometida con el desarrollo actual de la Internet.[83]

El nacimiento de la Internet en brazos del Pentágono

La desmesura de la Guerra Fría fue la madre de las tecnologías que sostienen la llamada "sociedad red"[84] o "sociedad de la información"[85], cuya columna vertebral es la Internet. En el

[82]CEO, del inglés Chief Executive Officer, es el encargado de máxima autoridad de la gestión y dirección administrativa en una empresa, organización o institución.

[83] "*La investigación Militar: la cara oculta de la ciencia*". Campaña "*Por la Paz: No a la investigación militar*", Madrid, febrero de 2005.

[84] Castells: obra citada.

contexto del enfrentamiento de las dos grandes potencias mundiales**,** las inversiones en tecnología y ciencia avanzadas fueron decisivas para mantener la presión económica y militar sobre la economía de la URSS, que finalmente no resistió el margen de competencia. En Estados Unidos, estas inversiones recibieron un abrumador apoyo del gobierno y de la opinión pública, especialmente desde que el supuesto reto del programa espacial soviético se convirtiera en una "amenaza" para la seguridad nacional estadounidense.

En 1958 la administración Eisenhower creó el Servicio de Proyectos de Investigación Avanzada del Departamento de Defensa (Defense Advanced Research Projects Agency, el mítico DARPA), en respuesta al lanzamiento un año antes del satélite orbital Sputnik. La orientación de DARPA fue muy clara: encontrar y desarrollar rápidamente la tecnología avanzada de las Fuerzas Armadas para que los Estados Unidos no volvieran a sufrir una sorpresa tecnológica de ninguna otra nación. Inicialmente la agencia DARPA se concentró en los proyectos espaciales, produjo el cohete Saturno V-que permitió a los Estados Unidos lanzar la misiones Apollo a la Luna- y los primeros satélites de vigilancia, que se concentraron en espiar a los soviéticos, en particular su programa de misiles. DARPA dirigió el proyecto que desarrolló ARPANET, la primera experiencia tecnológica de la Internet mundial, una arquitectura que no podía ser controlada desde ningún centro, compuesta por miles de redes informáticas autónomas que tienen modos innumerables de conectarse, sorteando las barreras electrónicas.

"DARPA desempeñó en los Estados Unidos un papel muy similar al del MITI[86] en el desarrollo tecnológico japonés, incluido el diseño y la financiación inicial de la Internet"[87]. En la década del 80, cuando el gobierno de Reagan sintió la amenaza de la competencia japonesa, el Departamento de Defensa financió SEMATECH, un consorcio de empresa electrónicas norteamericanas, para apoyar costosos programas de I+D en la fabricación electrónica por razones de seguridad nacional. El gobierno federal también invirtió a favor de que cooperaran entre sí varias empresas de la microelectrónica que se integraron finalmente en el MCC, ubicando SEMATECH y MCC en Austin (Texas). Entre 1950 y 1960, los contratos militares y el programa espacial resultaron mercados esenciales para la industria electrónica, tanto para los gigantescos contratistas de defensa de California del Sur como para los innovadores que se acababan de poner en marcha en Silicon Valley y Nueva Inglaterra. "No podrían haber sobrevivido –afirma Castells[88]- sin la generosa financiación y los mercados protegidos de un gobierno estadounidense ansioso por recobrar la superioridad tecnológica sobre la Unión Soviética, una estrategia que acabaría siendo rentable."

DARPA se organizó en forma independiente de la comunidad de investigación y desarrollo militar. Su misión consistía en desarrollar y proveer aplicaciones tecnológicas no convencionales para la defensa de EE.UU. ampliando la frontera tecnológica a favor de una organización reducida en número, pero flexible, libre de condicionamientos y dotada de científicos de elite. Estaba formada por científicos universitarios, sus colegas y los alumnos de sus colegas, y consiguió generar una red de contactos fiables en el mundo universitario, así como en los centros de investigación surgidos de las universidades para trabajar para el gobierno. La comprensión

---

[85] Machlup, Fritz.: *The Production and Distribution of Knowledge in the United States*. Princeton, NJ: Princeton University Press, 1962.

[86] Ministerio de Industria y Comercio Exterior del Japón (MITI).

[87] Stowsky, Jay: "*Secrets to shield or share? new dilemmas for military R&D policy in the digital age*". Goldman School of Public Policy, University of California. 14 February 2003.

[88] Castells: ob.cit, p.103

cabal de cómo funciona realmente la investigación llevó a la agencia DARPA a conceder una considerable autonomía a los investigadores contratados o financiados por la agencia, condición *sine qua non* para que los investigadores realmente innovadores aceptasen involucrarse en un proyecto.

El cálculo estratégico de DARPA era que una colosal inversión de recursos en función de la innovación científica, necesariamente conduciría a algo bueno, de lo cual pudieran beneficiarse las Fuerzas Armadas y por extensión, la economía norteamericana. Fue una estrategia adecuada, incluso en términos militares. Su otro presupuesto ha sido ir más allá de las necesidades y requerimientos conocidos en el presente. Como han evaluado historiadores militares, "la propuesta de DARPA es imaginar qué capacidades pudiera desear un comandante militar en el futuro, y acelerar estas capacidades de forma concreta a través de demostraciones tecnológicas. Esto no sólo proporciona opciones al comandante, sino que también cambia la mentalidad acerca de lo que es tecnológicamente posible hoy en día."[89]

Adicionalmente, la elite política y militar reconoció la necesidad de una organización de alto nivel del Departamento de Defensa que formulara y ejecutara proyectos de I+D que expandieran las fronteras de la tecnología más allá de los requerimientos inmediatos y específicos de los servicios militares y de sus laboratorios. Para cumplir esta misión, ARPA desarrolló y transfirió programas de tecnología que abarcaban una gran variedad de disciplinas científicas. La clave esencial era convertir de manera inmediata cada proyecto de investigación en pura aplicación, un esfuerzo cuyo impulso institucional venía cuajándose desde 1940 con la Oficina de Investigación Científica y Desarrollo -creada por Franklin Roosevelt antes de que los Estados Unidos se involucraran en la Segunda Guerra Mundial[90]- y que fuera favorecido además por la cada vez

Reducción del tiempo entre invención y aplicación			
Producto tecnológico	**Año de invención**	**Año de producción**	**Tiempo de desarrollo**
Luz fluorescente	1852	1934	82 años
Radar	1887	1933	46 años
Pluma de punto rodante	1888	1938	50 años
Cremallera para ropa	1891	1923	32 años
Papel celofán	1900	1926	26 años
Cohetes	1903	1935	32 años
Helicóptero	1904	1936	32 años
Televisión	1907	1936	29 años
Khodachrome	1910	1935	25 años
Transistor	1940	1950	10 años

[89] Chambers, John: *The Oxford Companion to American Military History*. Oxford University Press, New York, 1999. p.791

[90] La Oficina de Investigación Científica y Desarrollo (OSRD por sus siglas en inglés) fue creada para garantizar que la industria orientara sus esfuerzos de investigación al armamento y los requerimientos militares. Tradicionalmente el sistema militar demandaba ingeniería y producción, pero no investigación básica. De manera que la OSRD fue la primera que se encargó de la investigación básica. Esta relación entre ciencia y tecnología, e intereses militares quedó así clara por primera vez en la historia de los Estados Unidos (*Air Force Office of Scientific Research, "AFOSR at 50: Five Decades of Research that Helped Changethe World," Research Highlights, Mar/Apr 2002, 1. Se puede descargar en* *http://www.afosr.af.mil/Documents/ResearchHighlights/pub_2002MarApr.pdf*

menor distancia temporal entre las llamadas ciencias básicas y su aplicación práctica en los mercados. [91]

La evolución de la Internet es tal vez el caso clásico de un proyecto militar de inversión I+D, organizado a partir de esfuerzos compartidos de innovación entre el ámbito militar y civil que evolucionó, sin embargo, en un ambiente protegido por el Pentágono. En el caso de la Internet, el desarrollo de la tecnología patrocinada originalmente por DARPA fue posible cuando se incorporaron al grupo inicial del Departamento de Defensa investigadores de las universidades y de otros laboratorios de gobierno.

A principio de los años 60, la idea flotaba entre diversas instituciones norteamericanas, como el Massachussetts Institute of Technology (MIT) y la corporación militar RAND. Leonard Kleinrock del MIT publicó en julio de 1961 el primer trabajo sobre "conmutación de paquetes" (la tecnología que permitía dividir los datos y que recorrieran rutas distintas). El Pentágono, a través de DARPA financió la puesta en marcha de una prueba práctica. En 1969, el año que el hombre llegó a la Luna, se abría el primer nodo de la red ARPANET, en la Universidad de California en Los Ángeles.

El segundo nodo fue el del Stanford Research Institute (SRI), donde trabajaba Douglas Engelbart en un proyecto sobre "Ampliación del intelecto humano", en el que también estaban interesados los militares. Engelbart había inventado el ratón para computadoras un lustro antes, y se preocupaba por el trabajo en colaboración a través del hipertexto. No era un visionario aislado. En el MIT, J.C.R. Licklider ya discutía en 1962 su concepto de "Red Galáctica": un conjunto de computadoras interconectados para dar acceso a almacenes de datos. De modo que esta red, en la que participaban distintos centros de investigación, empezó a servir para algo realmente revolucionario: para comunicar personas, más que computadoras. En 1969 apareció en la Universidad de California en Los Ángeles el sistema de RFC (Request for Commentaries: petición de comentarios), que permitía a todos los participantes en el proyecto opinar sobre las temas técnicos. En 1972 -fecha de la demostración pública de la red- apareció el primer programa de correo electrónico, que pronto se convirtió en una de las aplicaciones más usadas, mientras el primitivo proyecto ARPANET se preparaba para unirse con otras redes: de satélite (el primero comercial se había lanzado en 1962), de radio terrestre, y de otros tipos, siempre y cuando compartieran la conmutación de paquetes. Robert Kahn introdujo esta "arquitectura abierta" en 1972: se la llamó Internetting, porque servía para la relación entre redes (net, en inglés).

En 1983 se creó el sistema de nombres de dominios (.com, .edu, etc., más las siglas de los países), que prácticamente se ha mantenido hasta ahora. En la constitución y crecimiento de esta nueva "red de redes" -que pronto contó con nodos en Europa-, las agencias federales norteamericanas, particularmente el Pentágono, volvieron a intervenir para financiar su infraestructura e impusieron las normas técnicas y jurídicas que despejarían el camino para clonar las leyes sobre seguridad, de modo que las tecnologías de la información se convirtieron en el cerebro y el sistema nervioso de todas las infraestructuras.

En 1984 William Gibson novelaba el nuevo mundo y acuñaba el término "ciberespacio". Al año siguiente se forjaba Well, la primera comunidad comercial de usuarios. ARPANET desapareció como tal en 1989, pero muchas instituciones (de la NASA al Departamento de Energía) ya habían creado sus propias redes, que podían comunicarse entre sí. El número de servidores en la red

[91] Burrus, D. and Gittines, R. *Technotrends*, Harper Business, New York, 1993. p. 81.

superaba los 100.000. Ese mismo año Tim Berners-Lee, investigador en el centro europeo CERN de Suiza, elaboró su propuesta de un sistema de hipertexto compartido: era el primer esbozo de la WWW. Como el ARPANET veinte años atrás, su propósito era poner en comunicación a los científicos, pero en 1992 -con más de un millón de servidores en la red- se creó la Internet Society, la "autoridad" de la red. Nacía como el lugar donde pactar los protocolos que harían posible la comunicación, bajo la mirada vigilante del gobierno de los Estados.

Con la extensión de las computadoras personales y el lanzamiento del primer navegador de la WWW popular, Mosaic, en 1993, ya había llegado el momento de "surfear la Web" (la expresión se registró por primera vez ese mismo año). Un chiste de Peter Steiner en New Yorker proclamaba: "En la Internet, nadie sabe que eres un perro". En 1994 se abrió el primer ciberbanco. En 1997 ya había 17 millones de servidores en la red y a partir de aquí las estadísticas se nublan: hoy uno de cada seis habitantes del planeta tiene acceso a Internet desde su casa y se pronostica que en el 2015 la mitad de la población mundial disponga de este servicio.

Esta revolución encabezada por Estados Unidos va desde los avances de la tecnología hasta algo más importante: la habilidad para vincular este desarrollo conjuntamente con la construcción de doctrinas, estrategias tácticas y tomar ventajas de su potencial técnico. En otras palabras, **la organización en Red está asociada a un pensamiento estratégico, que descansa en dos líneas fundamentales: la tecnológica y la puramente doctrinaria.**

La privatización de la Internet

A partir de la década del 90, sectores políticos entusiasmados con el curso que iban tomado estas tecnologías, propusieron la "modernización" de la doctrina imperial desde una visión decididamente electrónica[92]. No menos que los geoestrategas de la Guerra Fría, este grupo tenía su mirada fija en un mundo dirigido por los Estados Unidos, pero insistían con firmeza en que la forma de obtenerlo se basaba en el componente electrónico de la información y los medios de comunicación, que confiere poder cultural y poder en general.

David Rothkopf, uno de los principales funcionarios de la administración Clinton, en la actualidad director de su propio *think tank* –la Garten Rothkopf-, se mostró extraordinariamente entusiasta sobre sus expectativas para un futuro definitiva norteamericano basado en la información y la cultura extendida a través de estas tecnologías. En su ensayo "In Praise of Cultural Imperialism?", un clásico de la mentalidad escandalosamente imperial, asegura:

> *Inevitablemente, los Estados Unidos [son] la 'nación indispensable' en el manejo de los asuntos globales y el principal productor de productos informativos en éstos, los primeros años de la Era de la Información … Es interés político y económico de Estados Unidos asegurarse de que si el mundo se dirige hacia un idioma común, este sea el inglés; de que si el mundo se dirige hacia normas en materia de calidad, seguridad y telecomunicaciones comunes, éstas sean norteamericanas; de que si el mundo se está interconectando a través de la música, la*

[92] Schiller, Herbert I: "Augurios de supremacía electrónica global". Le Monde Diplomatique: Cuadernos de Información y Comunicación 2006, vol. 11 167-178

radio y la televisión, su programación sea norteamericana; y que si se están desarrollando valores comunes, sean valores con los que los norteamericanos estén cómodos.[93]

Rothkopf observa que estas "no son simples aspiraciones", sino realidades en vías de desarrollo: "La política de verdad para la Era de la Información pasa por establecer estándares tecnológicos, por definir estándares de programación, por producir los productos informativos más populares, y por liderar el desarrollo relativo a los servicios de comercio globales, de tal manera que sean esenciales para el bienestar de cualquier líder futuro como lo eran antes los recursos necesarios para mantener una industria o un imperio".[94]

Este proyecto para un país cableado y un mundo interconectado pasó del afiebrado discurso del asesor de Clinton a la realidad. Anunciada con autoridad presidencial en septiembre de 1993, la propuesta para una Infraestructura de Información Nacional (NII) se presentó como la respuesta electrónica completa a todo lo que necesitaba el país para dominar al mundo a través de estas tecnologías, con el apoyo entusiasta del Departamento de Defensa que seguía inyectando dinero en las universidades y en las empresas privadas.

Los beneficios fueron enumerados con un entusiasmo sin parangón: comunicaciones las veinticuatro horas del día para la familia; educación on-line proporcionada por los mejores maestros del país; acceso a los recursos artísticos, literarios y científicos globales; servicios médicos on-line para todos, sin esperas; trabajo desde casa; lo último en entretenimiento en tu sala de estar; fácil acceso a funcionarios gubernamentales y todo tipo de información on-line. Pero el requisito fundamental para todos estos beneficios fue una condición que, a la larga, sólo podía suponer la negación de los beneficios prometidos: la privatización de la Internet, que había sido desarrollada con fondos públicos: "El sector privado dirigirá el desarrollo de la NII [...] las empresas [son] las responsables de la creación y funcionamiento de la NII."[95]

De tal modo que esta tecnología de la información tan extraordinaria, desarrollada inicialmente con dinero del Gobierno, y operada ya entonces como servicio público, se entregó a un puñado de poderosas corporaciones de la comunicación —fabricantes de ordenadores, diseñadores de software, proveedores de servicios de telecomunicaciones y productores de medios de comunicación— para su desarrollo y expansión. La industria corporativa de la comunicación respondió a estas nuevas y potencialmente prometedoras oportunidades con un frenético proceso de fusiones y concentraciones, acumulando recursos y capital en enormes compañías.

Estas fueron acompañadas por una serie de subastas precipitadas de espectro radiofónico por parte del Gobierno, ganadas por los gigantes de las telecomunicaciones. Una vez aseguradas estas condiciones materiales, con los gigantes de la comunicación del sector privado preparados y alentados para explotar al máximo las recién nacidas redes digitales, la intervención gubernamental encaró otro asunto crucial: los mercados, en su mayoría extranjeros. Impusieron entonces el Framework for Global Electronic Commerce, un programa de política nacional cuyo principal objetivo fue internacional: dirigir el "comercio electrónico global", cuyo entorno político-económico no estaba todavía sometido a la voluntad de la Casa Blanca.

---

[93] Rothkopf , David: "In Praise of Cultural Imperialism?", Foreign Policy, n.º 107, verano 1997, pp. 38-53.
[94] Schiller, Herbert: Ob. cit.
[95] National Information Infrastructures (NII): Agenda for Action, Washington D.C., 15 de septiembre de 1993.

La resolución estableció que los intereses de las poderosas corporaciones dueñas de los derechos de propiedad intelectual prevalecen sobre los participantes más débiles en las transacciones. Advertía que "la nueva tecnología ha hecho posible el pago de bienes y servicios a través de Internet", lo que requiere "acuerdos internacionales que establezcan una protección clara y efectiva de los derechos de autor, patentes y marcas". Fue una de las primeras iniciativas de Washington para asegurarse el mejor trozo de la tarta del creciente flujo de comercio electrónico en el mercado mundial —que se origina fundamentalmente a partir de las operaciones de las compañías transnacionales- y para imponer las normativas internacionales al respecto.

A esto siguió la imposición a nivel mundial de la norma norteamericana para el ordenamiento de la red. Desde 1998 el gobierno de la Internet lo administra un ente supuestamente "híbrido", la ICANN (Internet Corporation for Assigned Names and Numbers), en cuyo consejo de administración se sientan 18 nacionalidades diferentes, pero que se rige por las leyes del estado de California. Sus funciones derivan de un contrato con el Departamento de Comercio norteamericano a tal punto que diez años después de la creación de esta entidad, la administración Bush sigue advirtiendo que en ningún caso renunciará a sus prerrogativas, ahora con el pretexto de la guerra contra el terror.

Un informe reciente patrocinado por 160 grandes corporaciones estadounidenses[96] elaboró un burdo pretexto para que el gobierno norteamericano siga maniobrando a su antojo en la ICANN: "Estados Unidos no está preparado para hacer frente a un ataque, accidente o desastre natural que pudiera afectar la infraestructura de Internet, una arteria vital para la seguridad y la economía de Estados Unidos". Por tanto, el Departamento de Seguridad Nacional ha organizado varios simulacros de respuesta a diversas amenazas, ejercicios que han sido bautizados como cyber Katrina y que, al parecer, han arrojado pobres resultados, pero el episodio sirve para ilustrar la preocupación de las autoridades de Washington cada vez que se menciona la posibilidad de recortar el control unilateral que ejercen sobre la gestión de Internet, para ellas estratégico.

Desde el punto de vista **tecnológico**, los militares siguieron desarrollando por su cuenta a niveles jamás vistos las comunicaciones electrónicas, los sistemas de vigilancia, los aviones no tripulados, los proyectiles dirigidos por satélites y un arsenal de aplicaciones de híbridos de la nanotecnología, la microelectrónica y la inteligencia artificial, que han permitido reducir la presencia física de los soldados en los escenarios bélicos o construir monstruos para el espionaje, como los insectos que se desplazan por GPS para la vigilancia de protestas antibélicas o la detección de campamentos enemigos. Las invenciones del tipo The Matrix, con su célebre cita filosófica "bienvenido al desierto de lo real", están cada vez más próximas a la realidad. *The New York Times*, por ejemplo, ha publicado lo siguiente:

> *El Pentágono predice que los robots serán una importante fuerza de combate en el ejército americano en menos de una década, y que perseguirán y eliminaran a nuestros enemigos en el campo de batalla. Los robots son una parte crucial del esfuerzo en el que está empeñado el Ejército para reformarse y convertirse en una verdadera fuerza de combate para el siglo XXI, y el contrato firmado para desarrollar un proyecto valorado en 127 mil millones de dólares y conocido como Sistemas de Combate del Futuro, es el contrato militar más importante de la historia americana. Los militares planean invertir decenas de miles de millones de dólares en unas fuerzas armadas completamente automatizadas..*[97]

[96] Se puede consultar en www.businessroundtable.org .
[97] *The New York Times*, 16 de febrero de 2005.

El ámbito de la **doctrina militar** norteamericana en Red es tan importante como el anterior. Un nuevo estilo de pensamiento está imponiéndose en los *think-tanks* militares de Estados Unidos y la OTAN. Se le conoce con el término de *swarming* [98]o enjambre y representa un cambio radical frente a las concepciones militares basadas en despliegues masivos de capacidad artillera, armamento blindado y grandes concentraciones de tropas. El enjambre es una estrategia militar en la cual una tropa ataca a un enemigo desde múltiples direcciones diferentes para después reagruparse.

Este tipo de guerra "no-lineal" elimina la noción del frente y representa una versión de alta tecnología de la guerra de guerrillas. La guerra "basada en redes", según la terminología del Pentágono, depende totalmente de un sistema de comunicaciones sólido y seguro, capaz de mantener una conexión constante entre todos los nodos de la red.

Estación del Comando del Ciberespacio, de la Fuerza Aérea norteamericana, en Luisiana. Esta fuerza, un nuevo Ejército que se incorpora a los ámbitos tradicionales de la guerra –la tierra, el aire y el mar-, estará en plenitud de facultades en octubre de este año y "se apoyará en estrategias militares que permitan interrumpir el sistema de comunicación enemigo, con mayor precisión que en Irak en el 2003, donde logramos intervenir todas las comunicaciones terrestres del Ejército de Sadam Hussein", como aseguró el General Robert Elder, jefe del Comando Ciberespacial.

Las implicaciones que esto está teniendo para las fuerzas armadas son enormes. Se ha ido desmontando paulatinamente la organización tradicional del ejército en cuerpos, divisiones, regimientos y batallones de gran envergadura. Lo mismo ha ocurrido con la división funcional entre diversas especialidades: infantería, unidades blindadas, comunicación, artillería, ingeniería. Las unidades han pasado a ser básicamente multifuncionales y dependen de su capacidad de conexión en red para conseguir apoyo mutuo.

En esta lógica surge el Comando Ciberespacial para el despliegue a través de las redes, que debe ser el responsable del incremento desmesurado de las agresiones contra sitios chinos y venezolanos en los últimos meses[99]. El Comando ciberespacial tiene una contraparte en el Departamento de Estado: el Grupo Especial de Tareas para la Libertad de la Internet Global (Global Internet Freedom Task Force, GIFTF, por sus siglas en inglés), una organización

[98] Literalmente, enjambre. El término procede del sustantivo **swarm** (enjambre), por tanto **swarming** sería un tipo de combate o ataque concentrado y ágil como de un enjambre de abejas.

[99] De acuerdo con los registros de la empresa norteamericana Akamai Technologies, líder en análisis del comportamiento del tráfico en Internet, estos dos países fueron los más atacados por "piratas" informáticos en el 2007. Para que se tenga una idea de lo que estamos diciendo: en julio de 2007 se implantó un récord. Venezuela, que posee 4 millones de usuarios de Internet, tuvo 764 ataques en 64 horas, 500 más que China, el país que seguía en la lista y que posee 200 millones de usuarios. En: http://www.akamai.com/html/technology/dataviz1.html

multiagencias subordinada directamente a Condoleezza Rice y dirigida por la subsecretaria de Economía, Comercio y Agricultura, de ese Departamento, Josette Sheeran Shiner. Este Grupo de Tareas, en el que participan agencias del gobierno, universidades e investigadores privados que "mantienen operativos las 24 horas del día", fue dado a conocer el 14 de febrero de 2006. En su segunda reunión de trabajo celebrada el 3 de abril de 2006, el GIFTF "discutió la práctica y construcción de estrategias para apoyar la libertad de Internet". Josette Shiner advirtió que en el encuentro donde participaron "altos" funcionarios del gobierno, "específicamente nos concentramos en los desafíos de la libertad de Internet en Irán, Cuba y China".

Como señala la RAND Corporation[100], "este proyecto doctrinal no puede ponerse en práctica sin un sistema de comunicación y vigilancia plenamente integrado. Esta nueva perspectiva requiere que las fuerzas armadas se transformen en una 'organización sensorial', en la que el sistema resultará fundamental para lograr mantener a las unidades operativas conectadas a la red. El sistema de mando, control, comunicaciones, ordenadores, inteligencia, vigilancia y reconocimiento (C4ISR) puede llegar a generar tanta información que será imprescindible... para mantener el *topsight* -una visión general de todo lo que esté ocurriendo-."

Por supuesto, sabemos que toda esta doctrina tiene una falla de origen: la subestimación del ser humano. Al final, toda guerra se decide en enfrentamientos cuerpo a cuerpo. No se puede ocupar el territorio, ni desarmar al enemigo, es decir, aniquilar su voluntad de lucha, sin vencerlo en el campo de batalla. Como dice Howard Zinn, "cuando Estados Unidos luchó en Vietnam, fue una confrontación entre tecnología moderna organizada y seres humanos organizados. Y vencieron los seres humanos."[101]

Movimientos sociales: pasar a la articulación horizontal

El Foro Social Mundial y las manifestaciones previas a la guerra de Iraq en el 2003, que incorporaron a millones de personas en todo el mundo, son ejemplos esperanzadores de las posibilidades de la conjunción de las redes técnicas con las redes sociales, desde el punto de vista que aquí analizamos. Pero habría que admitir que desde entonces no hemos vuelto a ver expresiones semejantes de resistencia política articulada.

Hasta el 2003, la falta de canales comunicativos estructurados resultó ser una fuerza y no una debilidad para las acciones de las redes contrahegemónicas, porque todos los movimientos podían ser inmediatamente eficaces y no esperaban ninguna clase de ayuda externa o extensión para garantizar su efectividad. Uno de los modelos más exitosos fue el de las movilizaciones contra la reunión de la OMC en Seattle, entre los días finales de noviembre y principio de diciembre de 1999.

Gracias a que todavía no estaban organizados los sistemas de vigilancia a través de la Red, desde múltiples puntos de la Internet se articuló la movilización, incluida una complicada logística –por ejemplo, la mayoría de los miles de participantes que llegaron a la ciudad no se alojó en hoteles para no llamar la atención de las autoridades, sino en la casa de otros activistas. Cuando el gobierno estadounidense se dio cuenta, la acción era ya un hecho. La célula matriz de las

[100] Arquilla, John, y Ronfeldet, David, "*Swarming and the future of conflict*", **RAND National Defense Research Institute**, Santa Mónica, CA, 2000.

[101] Zinn, Howard: *La otra historia de los Estados Unidos*. Editorial de Ciencias Sociales, La Habana, 2004. p.343.

protestas, los grupos de afinidad, eran unidades de 15 a 20 personas que funcionaban discrecionalmente y que tenían capacidad de tomar sus propias decisiones estratégicas. Algunos hicieron teatro callejero, otros se encadenaron, otros llevaban marionetas gigantes, algunos simplemente se agarraron de los brazos para impedir de manera no violenta el paso de los delegados. En cada grupo había gente dispuesta a ir a la cárcel, otros que serían el apoyo una vez que estuvieran en prisión y una persona calificada en primeros auxilios. La "descentralización coordinada", con el apoyo inestimable de Internet, hizo posible que se cumplieran los objetivos de la mayoría de los activistas, movilizados por todo el mundo.

Ya esto no se puede hacer sin desatar las alarmas. Se acabó el mito de que Internet era un espacio inmune a la regulación y como afirma Mike Davis, experto en ecología urbana y autor del libro *Planet of Slums* (Planeta de suburbios), "las mejores cabezas del Pentágono han aprendido la lección… Ahora tienen por blanco las ciudades salvajes, fracasadas del Tercer Mundo –especialmente sus suburbios marginados–, que serán el campo de batalla característico del siglo XXI. La doctrina bélica del Pentágono está siendo reformulada para apoyar una guerra mundial de baja intensidad de duración ilimitada contra segmentos criminalizados de los pobres urbanos."[102]

Desde mucho antes del 11 de Septiembre, la maniobra estadounidense sigue la pauta de adelantarse a cualquier otro gobierno o emporio global para ordenar la Red y proveerla de la arquitectura tecnológica, legal y represiva que mejor convenga a Estados Unidos. Cuenta con una circunstancia altamente beneficiosa para sus objetivos: la influencia de las políticas neoliberales, que fragmentan y atomizan las sociedades, e impiden que los grupos que enfrentan estas políticas reconozcan al enemigo principal. Al proyecto neoliberal le interesa que los grupos permanezcan aislados, enfrentados entre sí, sin capacidad de encontrar objetivos y estrategias comunes. Esta primera dificultad ha puesto en jaque la creación de redes de solidaridad y de comunicación antagónicas a la globalización neoliberal, porque choca con sus principios y con sus lógicas de funcionamiento.

La prueba es que un movimiento de extraordinaria importancia para la soberanía en la Red como el de la lucha por mantener la neutralidad en Internet[103], involucra casi exclusivamente a grupos por los derechos civiles en Estados Unidos. La ausencia de redes internacionales de solidaridad en torno a este tema y el desconocimiento de la ofensiva militar estadounidense en Internet, indican que las transnacionales de telecomunicaciones estadounidenses podrían alzarse con la victoria e imponer a todos más y más barreras para la libertad en Red. Sin ir demasiado lejos, en el discurso del 28 de enero sobre el Estado de la Nación, el presidente Bush prácticamente amenazó a los legisladores para que aprobaran de inmediato un nuevo proyecto de ley de vigilancia que le otorgaría inmunidad a las empresas de telecomunicaciones que colaboraron con el espionaje sin órdenes judiciales. Literalmente dijo: "Eso significa que si no toman medidas para el viernes, nuestra capacidad de permanecer al tanto de las amenazas terroristas se debilitaría

[102] Davis, Mike: *Planet of Slums*. Verso, Londres, marzo de 2006.

[103] La neutralidad de la Red era un principio que establecía que todos los sitios deben ser tratados de igual manera por los proveedores de servicio de Internet. Se encontraba recogida en la Ley de Comunicaciones estadounidense (Communications Opportunity, Promotion and Enhancement Act). Los movimientos sociales norteamericanos han ido perdiendo, una tras otras, las batallas legales y políticas por la defensa de este principio que convertiría a la Red en una autopista de doble estándar: uno para los ricos que puedan pagar servicios exclusivos de banda ancha, y otro para los pobres, con prestaciones lentas y precarias.

y nuestros ciudadanos estarían en mayor peligro. El Congreso debe asegurarse de que no se interrumpa el flujo de inteligencia vital. El Congreso debe aprobar protecciones de responsabilidad legal a favor de las empresas que se considera que contribuyeron a los esfuerzos por defender a Estados Unidos. Tuvimos suficiente tiempo para debatir. Es hora de actuar."[104] Poco después la Ley se aprobó sin más dilación.

Es imposible controlar la Internet global, pero sí es posible controlar a la gente que la utiliza y, de hecho, estará cada vez más controlada, a no ser que se imponga un modelo que opte por la defensa de patrones solidarios y de transparencia de las instituciones, actuando desde las barricadas de los que exigen la libertad en el uso de Internet, pero yendo más allá de ellas en la confrontación con los mecanismos del poder político.

Además de todo el andamiaje de aparatos militares de ciencia ficción controlados gracias a estas tecnologías, Estados Unidos ha logrado producir sistemas que permiten el control de toda la población mundial. "Conocimiento total de la información" (Total Information Awareness: TIA, en inglés) es su nombre. Esto complementa –y supera con creces– la Red Echelon, la compleja trama de espionaje mantenida ilegalmente por los Estados Unidos y algunos de sus socios europeos, consistente en un tejido de antenas, estaciones de escucha, radares y satélites, apoyados por submarinos y aviones espía, unidos todos a través de bases terrestres, y cuyo objetivo es controlar todo tipo de comunicaciones mundiales, entre las que se encuentran correos electrónicos, envíos de fax, comunicaciones por cable, por satélite, transmisiones radiales, conversaciones telefónicas.

El dispositivo permite mantener un espionaje total, continuo y avasallador no sólo de las comunicaciones, sino también de las transacciones financieras, los registros de vuelo, las declaraciones de impuestos, la venta de paquetes accionarios, los movimientos de tarjetas de crédito, los archivos médicos y docentes de la población mundial. En definitiva: una forma de control absoluto de cada ser humano; control que se ejercerá sobre sus características biométricas (el tramado del iris, las huellas dactilares, la voz, sus hábitos motores como la forma de caminar)[105], todo lo cual permitirá un monumental banco de datos universales que posibilitará a los agentes de inteligencia buscar y hallar por satélite a una persona en cualquier lugar del mundo y con una velocidad pasmosa.

El nuevo sistema, desarrollado por el Comando de Inteligencia Naval de los Estados Unidos, consiste en una combinación de tecnologías de punta del campo de la informática, entre las que se cuenta una monumental base de datos que permite almacenar información personal de los 6300 millones de habitantes actuales del planeta, incluyendo vídeos, fotos y parámetros biométricos de cada ingresado al programa, con la capacidad de localización por satélite e

---

[104] Bush, George W., "Discurso del Presidente Sobre el Estado de la Nación". Cámara de Representantes de Estados Unidos, 28 de enero de 2008. Se puede descargar en el sitio http://www.whitehouse.gov/news/releases/2008/01/20080128-13.es.html

[105]" El ejército de los Estados Unidos está tomando huellas dactilares e imágenes oculares a miles de hombres iraquíes para crear una base de datos sin precedentes que los ayude a seguir la pista a sospechosos de ser militantes extremistas. Los efectivos estadounidenses están parando a los iraquíes en los puestos de control, centros de trabajo y lugares donde hayan ocurrido ataques recientes, e introducen los datos personales mediante el uso de escáneres de mano o computadoras portátiles especialmente equipadas. En varios vecindarios de Bagdad y sus alrededores, los efectivos han ido de puerta en puerta recopilando datos"(Frank, Thomas: "*Crean los EE.UU. base de datos sobre los iraquíes*". Usa Today, 13 de julio de 2007.)

identificación de seres humanos a distancia por medio de las características biométricas almacenadas.

Sumados todos estos elementos, el complejo mecanismo de espionaje –en palabras de Steven Wallach, antiguo ejecutivo en la empresa Hewlett-Packard y actual consejero del presidente Bush– "podrá asociar una foto de Malasia tomada por un satélite con una llamada realizada en Francfort y con un depósito bancario en Pakistán, para luego relacionar todos esos elementos con algo que pasará en Chicago".[106]

De modo que otro gran desafío de los movimientos alternativos será adquirir una conciencia de riesgo frente a estas realidades y trascender los modelos organizativos que dificultan la participación de sus miembros y la creación de redes con otros grupos. Seguimos aferrados a un modelo que se caracteriza por sistemas de difusión, al estilo de la televisión y de la radio, con un punto de emisión y muchos receptores que generalmente no son tenidos en cuenta. Estamos muy retrasados en el uso del modelo que propicia Internet, horizontal y desterritorializado.

Aún frente a tantos peligros, no se puede perder de vista que el futuro, al margen de la Red, no existe. A medida que Internet se va convirtiendo en la infraestructura dominante, la propiedad y el control del acceso a estas tecnologías se convierten también en el principal caballo de batalla político de la sociedad contemporánea. La lógica de la conexión de redes, que tiene su paradigma en la Internet, se ha hecho aplicable a cualquier ámbito de actividad, a cualquier contexto y a cualquier ubicación que pueda tener una conexión electrónica. La capacidad tecnológica, la infraestructura técnica, el acceso al conocimiento y recursos humanos calificados se han convertido en fuentes decisivas de la competitividad en el mundo actual, hasta el punto de que algunos teóricos afirman que tiende a desaparecer la noción de Tercer Mundo, a partir de la capacidad de algunos de los países de este grupo para producir servicios altamente competitivos en la economía global. (En los últimos años el informe de The Global Information Technology Report[107], preparado por el Foro Económico Mundial, muestra a Singapur a la cabeza de una lista de 104 países de todo el mundo en cuanto a crecimiento y aumento de la competitividad a partir del uso las tecnologías de la información y las comunicaciones. De acuerdo con el informe, debe su posición, entre otros parámetros, a sus avances en educación en las matemáticas y otras ciencias, bajas tarifas telefónicas y de acceso a Internet, y a la prioridad que su gobierno le asigna a las TIC.)

La realidad es que la evolución futura de la Red de Redes está sometida a las dinámicas contradictorias que oponen la dominación imperial a nuestros proyectos de justicia social y a nuestras esperanzas. El universo virtual es el espejo del universo tangible. Debemos situar nuestra acción en el contexto específico de dominación y liberación donde vivimos: en la sociedad red, construida en torno a las redes, y no al margen de ellas o creyendo ingenuamente que es el paraíso o el infierno, de acuerdo con el prisma con que se mire.

Manuel Castells reproducía un diálogo, en el que lo desafían del siguiente modo: "'¿Por qué no me deja usted en paz? ¡Yo no quiero saber nada de su Internet, de su civilización tecnológica, de su sociedad red! ¡Lo único que quiero es vivir mi vida!' Muy bien –respondió Castells-, pues si ese fuera su caso tengo malas noticias: si usted no se relaciona con las redes, las redes sí se

[106] Colussi, Marcelo: "Estados Unidos nos vigila". Rebelión, España, 29 de septiembre de 2006.

[107] http://www.weforum.org/en/initiatives/gcp/Global%20Information%20Technology%20Report/index.htm

relacionan con usted. Mientras quiera seguir viviendo en sociedad, en este tiempo y en este lugar, tendremos que tratar con la sociedad red."

A modo de conclusión

La red de redes no es solo una plataforma tecnológica. Es un nuevo espacio de interacción entre los seres humanos, que hemos creado nosotros mismos. Dicho de otro modo: las llamadas nuevas tecnologías de la información y comunicación no son solo herramientas, sino procesos que desarrollamos. Por primera vez en la historia ha aparecido un medio que le permite al ser humano ser a la misma vez usuario y creador de nuevas formas de relaciones y de nuevos medios con una misma herramienta.

Esta tecnología debe ser vista, analizada, manejada, estudiada y utilizada desde un punto de vista social, tratando de entender los nuevos tipos de relaciones que se establecen dentro de este espacio, los nuevos procesos sociales que genera, las transformaciones culturales que produce, las nuevas visiones de mundo que se construyen, las nuevas relaciones económicas que se establecen.

Marx comparó en su tiempo las luchas proletarias que emergían en la Europa del siglo diecinueve en términos de un topo y sus túneles subterráneos. Según él, "el topo de la resistencia" salía a la superficie en épocas de conflicto de clases abierto, y luego regresaba bajo tierra --no para hibernar pasivamente sino para cavar sus túneles, empujando hacia delante con la historia, de modo que cuando el tiempo fuese el adecuado (1830, 1848, 1870), saldría a la superficie nuevamente. "¡Bien escarbado, viejo topo!", decía Marx. Pues bien, el viejo topo de Marx ha sido sustituido por una serpiente que ondula en la superficie del planeta. Los túneles estructurados del topo han sido reemplazados. Las profundidades del mundo moderno y sus pasadizos subterráneos se han vuelto superficiales en la era de la globalización. Las luchas de hoy se deslizan a través de paisajes visibles gracias a la Red de Redes, una extraordinaria invención que debemos conocer a fondo si queremos transformar el mundo que vivimos.

La Internet no debe ser entendida solamente como la red de redes, desde un punto de vista técnico, es decir de máquinas interconectadas. La Internet debe ser vista como la red de redes humanas que se relacionan unas con otras y donde las computadoras son únicamente la plataforma tecnológica que permite mediatizar esas relaciones.

Está claro que el hecho de que se base en una plataforma tecnológica de computadoras interrelacionadas, hace que esta red de redes humanas funcione con características novedosas y particulares. Los sociólogos hablan de un nuevo modelo de sociabilización: las *heterarchies*, que es la articulación de redes sociales y redes técnicas para promover cambios radicales en la sociedad. Ejemplo: el Foro Social Mundial de Porto Alegre y las movilizaciones contra las reuniones de la OMC y la guerra en Iraq que llegaron a reunir en las protestas a millones de personas de todo el planeta. La ofensiva norteamericana en Internet, a partir del 2003, ha hecho que la característica fundamental de este tipo de expresiones de resistencias sea la fugacidad.

El gran reto de los movimientos contrahegemónicos, y en particular de un país como Cuba que puede asumir este desafío como voluntad de gobierno, es estudiar estas nuevas realidades y proveer alternativas para enfrentar la ofensiva imperial. La mala noticia es que el Imperio ha asestado duros golpes a estos movimientos y ha avanzado en sus estrategias de represión y control social utilizando estas mismas tecnologías. La buena noticia es que los millones de

personas que se alzaron contra la guerra y el neoliberalismo siguen viviendo en este planeta y están pendientes de una nueva señal para movilizarse de nuevo en Red.

Una alternativa semejante no se construye con voluntarismos, ni a partir de la observación empírica exclusivamente. En una sociedad estructurada en redes –como dice Ignacio Ramonet, "Globalización es neoliberalismo más Internet"-, debemos ser capaces de identificar las características esenciales de la era que vivimos. Solo conociendo a fondo la sociedad global podremos aportar soluciones para transformarla con un sentido liberador para el ser humano.

La Internet es sobre todo una herramienta apta para crear y reforzar las redes humanas. Todos los analistas, de derecha y de izquierda, críticos y acríticos de la red de redes, coinciden en que son dos las premisas esenciales para poder construir nuestra alternativa en la sociedad en red:

- la alfabetización digital
- la extensión social de la red.

Por educación digital debe tenerse en cuenta, además de la capacitación en el uso de plataformas de software y de la Internet en particular, el conocimiento del entorno político, económico, social, cultural, lingüístico, infoecológico, ético, organizativo… en que se produce la revolución de las nuevas tecnologías de la información y la comunicación. Un programador que desconozca la sociedad donde evoluciona esta tecnología cuyo uso no es neutral, es tan analfabeto e imprudente como el funcionario que toma decisiones en nombre de una colectividad, ignorando la lógica de la sociedad en red donde esta vive. Educación digital supone que todos, desarrolladores y expertos en estas tecnologías, actores políticos y usuarios convencionales adquieran, junto con los aspectos metodológicos del uso de la red, una ética y una cultura para este tipo de relaciones de acuerdo con nuestro modelo histórico.

Tabla-ESTADISTICAS MUNDIALES DEL INTERNET Y DE POBLACION

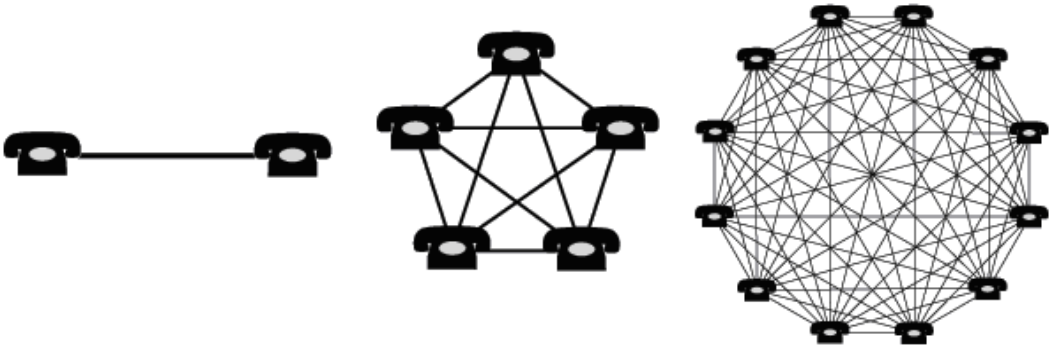
Regiones	Población (2007 Est.)	% Población Mundial	Usuarios	% Población (Penetración)	Crecimiento 2000-2007
Norte América	334,538,018	5.1 %	234,788,864	70.2 %	117.2 %
Oceanía / Australia	34,468,443	0.5 %	19,039,390	55.2 %	149.9 %
Europa	809,624,686	12.3 %	337,878,613	41.7 %	221.5 %
Latinoamérica / Caribe	556,606,627	8.5 %	115,759,709	20.8 %	540.7 %
Oriente Medio	193,452,727	2.9 %	33,510,500	17.3 %	920.2 %
Asia	3,712,527,624	56.5 %	459,476,825	12.4 %	302.0 %
África	933,448,292	14.2 %	43,995,700	4.7 %	874.6 %
TOTAL MUNDIAL	6,574,666,417	100.0 %	1,244,449,601	18.9 %	244.7 %

Es imposible potenciar los procesos de desarrollo humano sin la ampliación de la conectividad, es decir, sin la extensión social a gran escala de las redes tecnológicas. Cuba es el único país del mundo que padece el bloqueo del acceso a la Red internacional impuesto de manera inflexible por el gobierno norteamericano, que ha decretado la exclusión del país de este ámbito esencial de desarrollo y participación política. Saben que quien no esté ahí a la vuelta de unos pocos años, no existirá ni tendrá posibilidades de influencia en un mundo donde la lógica es extender al máximo posible la red tecnológica para controlar los mercados, presentándolo incluso como gesto altruista hacia los países más pobres. Para que se tenga una idea de lo que esto significa, del año

2000 al 2007 el acceso a Internet en África creció un 874 por ciento y en el Medio Oriente más del 900 por ciento. [108]

La brecha digital que hoy se está configurando es la del acceso a los servicios de valor agregado, fuente de las máximas ganancias, más que de extensión de la red, que abarata cada vez más los costos y garantiza la reproducción y ampliación de las necesidades de esos servicios. En un futuro no muy lejano, la brecha entre conectados y desconectados será mayor que la conocemos hoy entre ricos y pobres.

Robert Metcalfe, el creador de la tecnología de la red de área local (Local Area Network, LAN), un modo de interconexión de computadoras, propuso en 1973 una sencilla fórmula matemática que mostraba cómo el valor (V) de la red aumenta con el cuadrado del número de nodos (n) de la red: $V=n^{(n-1)}$. Y que se representa gráficamente de la siguiente manera:



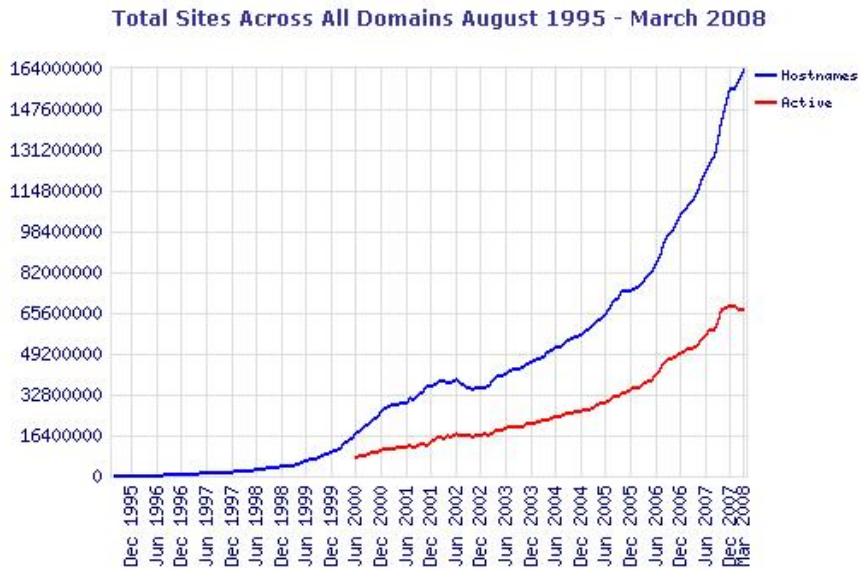
Es decir, a mayor ampliación de la red, los beneficios de estar en ella se incrementan de forma exponencial, mientras que los costos de exclusión de la red aumentan con el crecimiento de la Internet global debido al número decreciente de oportunidades de alcanzar conocimiento y servicios esenciales fuera de esta[109]. Lo mismo ocurre con los contenidos en la web: a mayor cantidad de seres humanos conectados, mayor será el número de páginas web y sus variables, y mayores las posibilidades de visibilidad de la expresión de un país, con sus virtudes y defectos. A pesar de los grandes esfuerzos que se han hecho por extender nuestra presencia en la Internet, la realidad es que Cuba está en la cola de los países en la región, en cuanto a cantidad de dominios de nivel superior (internacionales y nacionales)[110] del mundo, lo que se traduce en escasa presencia de medios en la web. Según el último reporte público del LACTLD, entidad que regula los Nombres de Dominio y Números IP en América Latina y el Caribe, el 31 de mayo de 2008 el

[108] Las estadísticas pertenecen a www.exitoexportador.com .

[109] Castells: Ob.cit. p.104.

[110] Los dominios en Internet son la variante para el ciberespacio del código postal: es un nombre base que agrupa a un conjunto de equipos o dispositivos y que permite proporcionar nombres más fácilmente recordables en lugar de las direcciones numéricas (IP) que identifican a las computadoras en red. Cada país tiene su dominio nacional, que en el caso de Cuba es .cu (punto cu). El 11% de dominios no tienen un sitio, el 65% posee múltiples páginas, y el 23% de los dominios tiene una página única., de acuerdo con una reciente investigación de Verising, A un nombre de dominio pueden estar asociadas varios sitios web o secciones de esa misma familia. Por ejemplo, al dominio cubaweb.cu están asociados los sitios www.granma.cubaweb.cu, www.jrebelde.cubaweb.cu, etc… (La estadística a la que hago referencia puede consultarse en http://www.latinoamericann.org/modules.php?op=modload&name=News&file=article&sid=1649)

país tenía registrados 1466 dominios .cu. Por debajo de la Isla en la región se encuentran Guyana, Haití y Barbados, países que usan más los dominios internacionales que los de sus propios países, a la inversa de Cuba. [111].



Es fácil deducir que, si queremos romper el cerco norteamericano que nos desconecta del mundo para multiplicar por cero nuestra influencia, Cuba debe buscar urgentemente alternativas de extensión de la red nacional y de interconexión internacional, incluso antes de que se concrete el proyecto del cable submarino que enlazará Siboney y La Guaira.

Las nuevas tecnologías de la información y la comunicación no son buenas ni malas por sí mismas. Si le damos un uso humanista facilitará la reestructuración de las relaciones sociales en función de un modelo basado en la solidaridad. Ese es nuestro principal objetivo: extender ese modelo hasta donde nos sea posible y más allá, y ayudar a resolver necesidades concretas de los seres humanos, con la conciencia de que, al ser un reflejo de las relaciones del mundo en que vivimos, la Internet también puede tener consecuencias negativas en la vida personal, organizativa y social.

No debemos exagerar su trascendencia en el mundo de hoy. La Internet es una fuente interminable de información, pero no nos provee conocimiento. El conocimiento lo producimos nosotros en forma individual o colectiva al asimilar la información, reflexionar sobre ella, adaptarla a nuestras experiencias, necesidades, condiciones, visiones de mundo, al discutirla con otros en forma presencial o en forma virtual.

La generación de conocimiento implica desarrollar el "proceso de pensar" y esta es una acción de carácter absolutamente humano. La Internet nos ayuda en este proceso y nos lo facilita porque encontramos dentro de ella experiencias similares, lecciones aprendidas, nuevas ideas sobre lo mismo, recibimos aportes, ampliamos nuestras visiones, discutimos ampliamente con personas y grupos de muchas partes del mundo. Pero, el proceso de generación de conocimientos sucede

[111] De acuerdo con el medidor internacional Web Metrics, Cuba tiene un total de 2 008 dominios registrados, incluyendo los nacionales e internacionales. En marzo de 2008, había registrados 164 millones dominios internacionales en todo el mundo: el 0,001 % es de Cuba. http://www.webometrics.info/Size_by_Domain_World.asp?offset=50

fuera de la Internet. De modo que seamos cuidadosos al asegurar que basta con proponérnoslo para construir una nueva sociedad de la información y el conocimiento. Podemos estar repitiendo una consigna. Como mismo hay que superar cierta paranoia de que todo lo que viene por ahí puede ser nocivo y lo que no entiendo no lo promuevo o no existe, es necesario superar el mito de que la información es conocimiento y que, por consiguiente, el solo hecho de estar conectado a la red me da más libertad y más cultura.

Por otro lado, no podemos ignorar que el desarrollo de estas tecnologías se produce en un entorno de profundas desigualdades. El grupo Estados Unidos, Japón y Alemania tiene un por ciento de la población mundial similar al de América Latina, pero la inversión en investigación desarrollo es de 52,9 por ciento frente a 1,3 por ciento. El mercado global para las Tecnologías de la Información y las Comunicaciones (TIC) alcanzó tres millones de millones de dólares norteamericanos en el año 2006, que fueron a parar a unos pocos países y a Estados Unidos en particular.

Las tendencias a la privatización del conocimiento y a la internacionalización de la investigación científica en empresas subordinadas al gran capital ha ido creando una especie de "Apartheid científico" para la gran mayoría de la humanidad. La Organización Internacional del Trabajo (OIT) indica que el número de los científicos e ingenieros que abandonan sus países de origen hacia naciones industrializadas equivale a cerca de un tercio del número de los que se quedan en sus países de origen, lo cual provoca una merma importante del capital humano indispensable. El robo de cerebros no es concepto abstracto, sino el día a día de una de las formas más brutales de exclusión de los países del Tercer Mundo de todas las posibilidades de desarrollo.

Para detectar nuestro propio horizonte, hay que estudiar científicamente, sistemáticamente y desde perspectivas multisectoriales –como el Grupo Especial de Tareas para la Libertad de la Internet Global, del cual ya hablamos–. Seguir críticamente lo que se están produciendo en el ámbito científico internacional y nacional para poder asegurar que no estemos más bien reforzando las estructuras existentes y garantizar que la transformación que desde este país se pueda producir será verdaderamente sustancial. Hay una gran diferencia entre el uso y el **uso con sentido** de esta herramienta tecnológica, que permite la apropiación social y la expresión ética en el ciberespacio, frente a modelos que apuestan por una ciencia y una tecnología crecientemente militarizadas.

El diseño del modelo de la Internet cubana necesita de una institución que dote al país de una mirada integral y crítica de lo que en este ámbito ocurre, que analice los muchos factores y dinámicas que transforman la red permanentemente, que ayude a trazar las políticas y las normativas, que identifique ágilmente las acciones del enemigo y ayude a modelar las alternativas, que dote de un instrumental científico que nos permita pasar a la ofensiva.

Además de la conciencia de riesgo que nos permite tomar decisiones con conocimiento de causa, habría que reforzar el sentido de la urgencia. Cada minuto que perdamos es tiempo que no se recupera. No se puede construir una cultura digital en unos pocos meses y el Imperio no va a esperar pacientemente a que nosotros nos desarrollemos en condiciones de normalidad. A marcha forzada se acerca la ofensiva del Pentágono y de las fuerzas que quieren convertir la Internet en una red donde una mayoría termine atrapada para que acate el modelo imperial. Cuba debe proponer soluciones al país y al mundo a más tardar hoy.

VII- Las redes sociales. Oportunidades y amenazas para la Seguridad nacional de Cuba

Ninguna otra invención humana ha sido la responsable de acortar tan dramáticamente los tiempos históricos. Ninguna otra ha pasado tan rápidamente del laboratorio a la sala de la casa del ciudadano común. No se conoce alguna similar que haya penetrado tan sensiblemente todos los reinos de actividad humana a escala planetaria. Hasta los neurocientíficos nos están diciendo que la Internet está cambiando el desarrollo de nuestro cableado cerebral en la infancia y la adolescencia, y que ya no somos los mismos desde que las redes humanas se montaron en el zeppelín de las redes tecnológicas.

Con la Internet también estos procesos complejos de interacción entre grupos de individuos –redes sociales, que existen desde que el hombre aprendió a vivir en comunidad-, han terminado mimetizados en herramientas. En parte porque estas son cada vez más comunes debido a la extraordinaria penetración de la red tecnológica. Y en parte, también, por la capacidad que tiene la Internet para reproducir simbólicamente el mundo físico y los diversos lenguajes y sensaciones que intervienen en la comunicación humana.

De hecho, si hiciéramos un poco de abstracción es fácil reconocer los espacios que replican de manera simbólica cada una de estas herramientas y nichos virtuales: la web sería el estanquillo de la esquina y la biblioteca; el blog, el diario de la adolescente; Facebook, la discoteca; Twitter, radio-bemba…

LA TEORÍA DE LA RED SOCIAL

La red social es exactamente lo que solíamos imaginar cuando nadie conocía el correo electrónico o la web: estructura sociales compuestas de grupos de personas, conectadas por uno o varios tipos de relaciones -la amistad, el parentesco, los intereses y los conocimientos comunes.

En el lenguaje cotidiano se ha utilizado libremente la idea de "red social" durante más de un siglo para denotar conjuntos complejos de relaciones entre miembros de los sistemas sociales en todas las dimensiones, desde el ámbito interpersonal hasta el internacional. Pero en 1954, el antropólogo de la Escuela de Manchester J. A. Barnes comenzó a utilizar sistemáticamente el término para mostrar patrones de lazos, abarcando los conceptos tradicionalmente utilizados por los científicos sociales: grupos delimitados (tribus, familias) y categorías sociales (género, etnia)[112].

La arquitectura del software de las redes sociales en Internet parte de la teoría de los “seis grados de separación”, según la cual toda la gente del planeta está conectada a través de no más de seis personas. De hecho, existe una patente en EEUU conocida como *six degrees patent*[113] por la que ya han pagado Tribe y LinkedIn, dos herramientas para reforzar las redes sociales. La teoría fue inicialmente propuesta en 1929 por el escritor húngaro Frigyes Karinthy en una corta historia llamada *Chains.*[114]

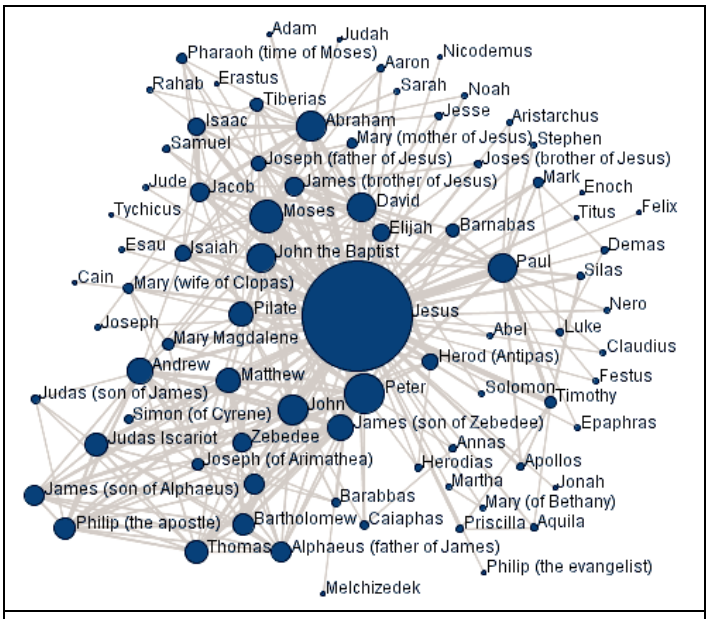
---

[112] Linton Freeman, *The Development of Social Network Analysis.* Vancouver: Empirical Press, 2006.

[113] Es la Patente número 5263382 de los Estados Unidos. Fue publicada el 23 de noviembre de 1993. Puede descargarse en http://www.freepatentsonline.com/5263382.html

[114] Notas biográficas en Wikipedia y una selección de artículos sobre esta obra. En: http://en.wikipedia.org/wiki/Frigyes_Karinthy

El concepto está basado en la idea de que el número de conocidos crece exponencialmente con el número de enlaces en la cadena, y sólo un pequeño número de enlaces son necesarios para que el conjunto de conocidos se convierta en la población humana entera.



Red social que reproduce los grados de relaciones entre los personajes de la Biblia

Según esta teoría, cada persona conoce de media, entre amigos, familiares y compañeros de trabajo o escuela, a unas 100 personas. Si cada uno de esos amigos o conocidos cercanos se relaciona con otras 100 personas, cualquier individuo puede pasar un recado a 10 000 personas más tan solo pidiendo a un amigo que pase el mensaje a sus amigos.

Estos 10 000 individuos serían contactos de segundo nivel, que un individuo no conoce pero que puede conocer fácilmente pidiendo a sus amigos y familiares que se los presenten, y a los que se suele recurrir para ocupar un puesto de trabajo o realizar una compra. Cuando preguntamos a alguien, por ejemplo, si conoce una secretaria interesada en trabajar estamos tirando de estas redes sociales informales que hacen funcionar nuestra sociedad.

Este argumento supone que los 100 amigos de cada persona no son amigos comunes. En la práctica, esto significa que el número de contactos de segundo nivel será sustancialmente menor a 10 000 debido a que es muy usual tener amigos comunes en las redes sociales. Pero si esos 10 000 conocen a otros 100, la red ya se ampliaría a 1 000 000 de personas conectadas en un tercer nivel, a 100 000 000 en un cuarto nivel, a 10 000 000 000 en un quinto nivel y a 1 millón de millones en un sexto nivel. En seis pasos, y con las tecnologías disponibles, se podría enviar un mensaje a cualquier individuo del planeta.

Evidentemente cuanto más pasos haya que dar, más lejana será la conexión entre dos individuos y más difícil la comunicación. Internet, sin embargo, ha eliminado algunas de esas barreras: acorta los pasos entre los individuos al integrarlos, a partir de sus servicios para redes sociales mundiales.

En 1967, el psicólogo estadounidense Stanley Milgram ideó una nueva manera de probar la teoría de las redes, que él llamó "el problema del pequeño mundo"[115]. El experimento del mundo pequeño de Milgram consistió en la selección al azar de varias personas del medio oeste estadounidense para que enviaran tarjetas postales a un extraño situado en Massachusetts, situado a varios miles de millas de distancia. Los remitentes conocían el nombre del destinatario, su ocupación y la localización aproximada.

[115] Milgram, Stanley: "El Problema del Mundo Pequeño" En: Araucaria, vol. 4, Universidad de Sevilla, España, 2003. En http://redalyc.uaemex.mx/redalyc/pdf/282/28210402.pdf

Se les indicó que enviaran el paquete a una persona que ellos conocieran directamente y que pensaran que fuera la que más probabilidades tendría, de todos sus amigos, de conocer directamente al destinatario. Esta persona tendría que hacer lo mismo y así sucesivamente hasta que el paquete fuera entregado personalmente a su destinatario final.

Aunque los participantes esperaban que la cadena incluyera al menos cientos de intermediarios, la entrega de cada paquete solamente llevó, como promedio, entre cinco y siete intermediarios. De esta forma, y a pesar de que Milgram nunca utilizó personalmente el término *seis grados de separación*, sus hallazgos posiblemente contribuyeron ampliamente a la difusión y aceptación de dicho concepto.

Las redes sociales **no son estancas**, en el sentido de que un mismo individuo, grupo u organización puede considerarse miembro de diferentes redes sociales. Por ejemplo, un profesor de Universidad es parte de una red social definida por las relaciones de colaboración científica en proyectos de investigación con otros miembros de su Departamento. También puede considerarse otra red diferente de las relaciones de los profesores con los otros profesores con los que comparte asignatura. Pero ese mismo profesor puede considerarse miembro de otra red social en este caso definida por las relaciones entre profesores y estudiantes de una determinada carrera.

De modo que el concepto de red social es una herramienta conceptual para *abstraer una faceta o parcela de la realidad* que nos interesa como objeto de estudio y en la cual se observan relaciones entre entidades sociales. El **aspecto distintivo del análisis de redes sociales es que se fija en datos relacionales**, es decir, en los lazos o relaciones entre los integrantes de la red, sean estos individuos, grupos u organizaciones.[116]

En las ciencias informáticas, ha sido clave la teoría *del mundo pequeño* (a pesar de que no es llamado típicamente así) en el desarrollo de protocolos seguros *peer-to-peer (P2P)*, en los algoritmos de enrutamiento para Internet y redes inalámbricas, y en la búsqueda de algoritmos para redes de comunicación de todo tipo, particularmente aquellos servicios para redes sociales.

RED SOCIAL + SOFTWARE SOCIAL

En realidad lo que conocemos hoy por "Red Social" en Internet es la **web que refuerza las conexiones entre las redes sociales**. Ha habido una instrumentalización de la red social, confundiéndola con el servicio que presta a esa compleja estructura social una herramienta: el software social. Es trascendente no perder esta perspectiva, porque los caminos de lo que vulgarmente se conoce como "red social" en Internet están empedrados de confusiones, simplificaciones e

[116] En: http://es.wikibooks.org/wiki/Análisis_de_Redes_Sociales/Conceptos_Fundamentales

intentos de parcelar los foros sociales de acuerdo con los servicios que en un momento de su evolución ofrecen.

Seguir la evolución de estas herramientas nos permite entender que no es el instrumento el que define las asociaciones y la comunicación en esos espacios, sino la propia red social. De modo que pensar que Youtube, por ejemplo, es una web que sirve exclusivamente para que una comunicad intercambie videos, deja afuera la voluntad de los individuos que participan en ese espacio social para convertirlo en mucho más, de acuerdo con sus propias necesidades, las que crea el mercado, la fusión de las tecnologías, el azar, la aparición de nuevas plataformas multimediales, etc. Cinco años después de su aparición, Youtube ni se parece a sus orígenes: incluye foros, televisión de alta definición, televisión en vivo, transmisiones desde el espacio, geolocalización, servicios multiplataformas…, además del intercambio de video.

Los especialistas suelen identificar el origen de los servicios para redes sociales con la creación y desarrollo del proyecto Classmates.com, a cargo de Randy Conrads, el fundador de la empresa Classmates Online, Inc [117] en 1995. Él logró crear una plataforma tecnológica que puso en contacto a personas que coincidieron en el círculo infantil, en la escuela primaria, el instituto, colegios mayores, trabajo y hasta en el servicio militar.

En la actualidad, cuenta con más de 40 millones de personas entre Estados Unidos y Canadá, aunque está lejos de los más de 500 millones de Facebook (mes de julio de 2010), que ha tenido una expansión internacional más detallada y amplia que Classmates. Al incorporar el medio o plataforma tecnológica, esta web inauguró la era de los servicios para las redes sociales, formadas por:

- las Redes Sociales -conjunto de personas o individuos con alguna relación o interés común-
- las necesidades de comunicación
- el medio técnico o plataforma.

La extensión de estos servicios coincide con la maduración de la tecnología, y el paso de la llamada web 1.0 (la Internet como Biblioteca) a una versión más evolucionada, la web 2.0, con una gran capacidad replicante y de interconexión de servicios. El modelo 2.0 permite a la audiencia agregar contenido original por sí mismos.

Esta tecnología comienza su despegue en el 2002, cuando aparecen nichos para interconectar a amigos en línea en comunidades virtuales. Se hizo arrolladoramente popular en 2003, con la llegada de sitios tales como MySpace, surgida en los Estados Unidos, o Xing, en Alemania.

Al crecer la popularidad de estos sitios, las grandes compañías de Internet se abalanzaron sobre el espacio de las redes sociales en Internet. Google lanzó Orkut el 22 de enero de 2004. Otros buscadores como KaZaZZ! y Yahoo crearon redes sociales en 2005.

En estas comunidades, un número inicial de participantes envían mensajes a miembros de su propia red social invitándoles a unirse al sitio. Los nuevos participantes repiten el proceso, creciendo el número total de miembros y los enlaces de la red. Los sitios ofrecen características como actualización automática de la libreta de direcciones, perfiles visibles, la capacidad de crear nuevos enlaces mediante servicios de presentación y otras maneras de conexión social en línea.

[117] http://www.classmates.com/registration/index.jsp

En resumen, una red social pasa del contacto físico a otro ámbito ceñido por relaciones virtuales, que permiten compartir:

- Información
- Datos
- Imágenes y fotografías
- Vídeos
- Aficiones
- Grupos
- Noticias
- Amigos
- Comunidades Virtuales
- Ofertas/Demandas

Hay mucha literatura sobre este tema y múltiples segmentaciones, de acuerdo con los contenidos que se intercambian y las relaciones que se establecen, en el entorno de la Web 2.0, llegando a identificar a determinados portales de Internet como "redes sociales puras" –Facebook, MySpace y otras donde se fortalecen relaciones de "amistad".

El elemento común entre todas ellas son los llamados "software sociales", ese conjunto de herramientas de comunicación que hace posible la interacción y colaboración por medio de convenciones sociales. Estas herramientas engloban correo electrónico, lista de correo electrónico, grupos de noticias, mensajería instantánea, blogs, wikis, agregadores sociales, folcsonomía, así como cualquier otro tipo de comunidad virtual en red.

El término anglosajón –Social Software (SoSo)– apareció por primera vez en un artículo publicado en 1987 por Eric Drexler bajo el título *Hypertext Publishing and the Evolution of Knowledg*[118]. Entre las muchas definiciones que se han ensayado para el término, una que parece acercarse más es la de "software que soporta la interacción grupal" y el conjunto de "herramientas para facilitar la interacción y la colaboración, que dependen más de las convenciones sociales (en su uso) que de las propias funcionalidades que ofrecen".

El software social está construido a partir de una o más de las siguientes premisas:

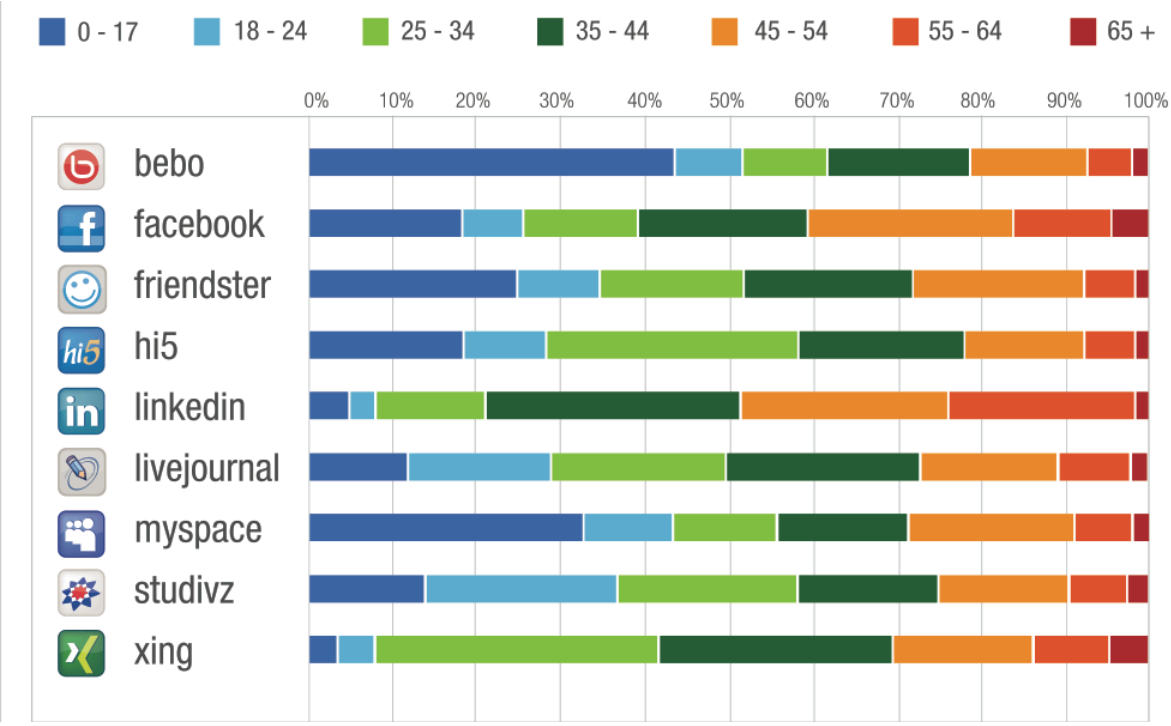
- Dar soporte a la interacción conversacional entre individuos o grupos –incluyendo conversaciones en tiempo real o diferido, e.g. mensajería instantánea y espacios de colaboración para equipos de trabajo, respectivamente [···]
- Dar soporte a la realimentación social –que permita a un grupo valorar las contribuciones de otros, quizás implícitamente, permitiendo la creación de una reputación digital [···]
- Dar soporte a las redes sociales –para crear y gestionar explícitamente una expresión digital de las relaciones personales de los individuos, así como para ayudarlos a crear nuevas relaciones [···]

[118] Drexler, K. Eric: *Hypertext Publishing and the Evolution of Knowledge.* Foresight Institute, Estados Unidos. En: http://www.islandone.org/Foresight/WebEnhance/HPEK1.html

O dicho de otra manera, estas herramientas operan en tres ámbitos, “las 3Cs”, de forma cruzada:

- Comunicación (nos ayudan a poner en común conocimientos).
- Comunidad (nos ayudan a encontrar e integrar comunidades).
- Cooperación (nos ayudan a hacer cosas juntos).

El software social es una metáfora que hace referencia a métodos de organización que favorecen la integración de las personas, la información en distintos soportes, el trabajo y la tecnología[119]. Es un espacio señoreado por los llamados nativos digitales, aquellos que nacieron cuando ya que existía la tecnología digital, y por tanto esos elementos siempre fueron parte de su vida.[120]



Los métodos populares combinan ahora muchos tipos de servicios: MySpace y Facebook son los más utilizados en América del Norte; Bebo,MySpace, Skyblog, Facebook, Hi5 y Tuenti en partes de Europa; Hi5, Sonico , Orkut y Muugoo en América del Sur y América Central; Friendster, Orkut y CyWorld en Asia y las Islas del Pacífico y LiveJournal en Rusia.

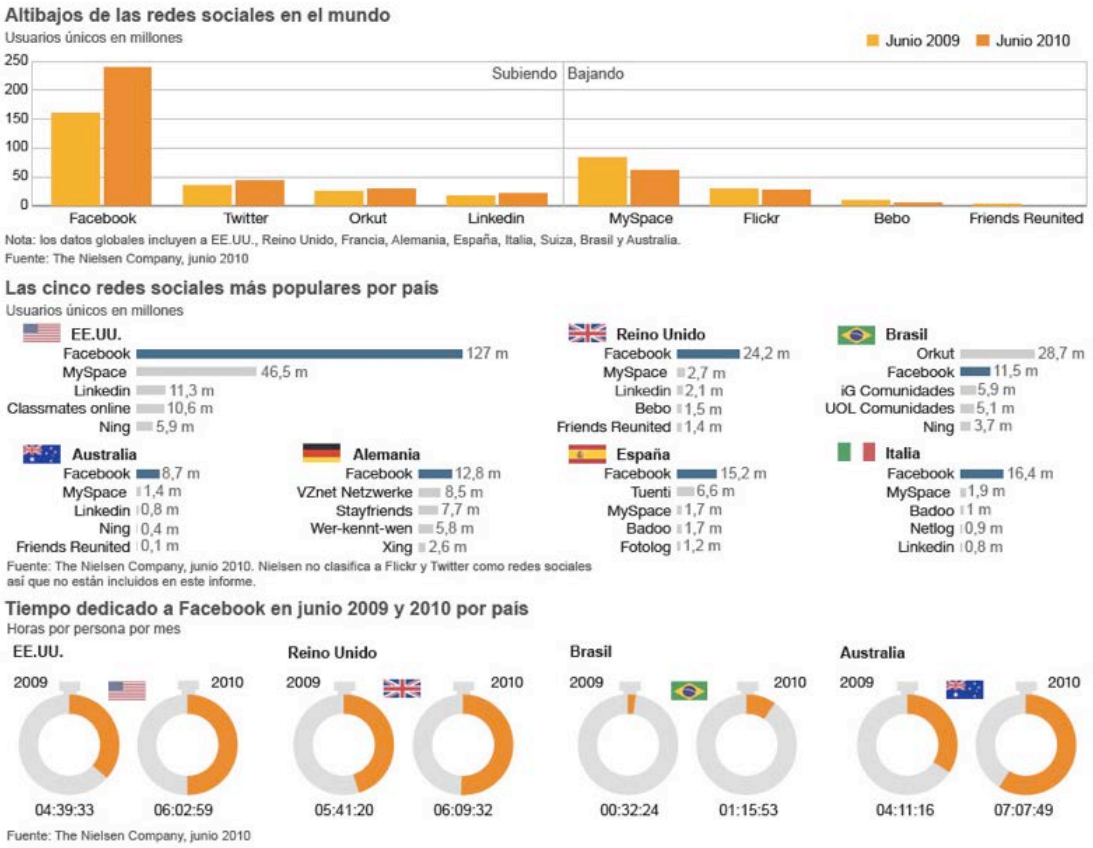
[119] Fumero, Antonio; Roca, Genís: *Web 2.0*. Fundación Orange, España. 2007. En: http://www.scribd.com/doc/65551/Libro-Web-20

[120] El término fue acuñado por Marc Prensky, en su libro *Nativos Digitales*, publicado en el 2001. Ubica como nativos digitales aquellos que nacieron a partir de finales de la década del 70, momento en comenzaron a socializarse las llamadas nuevas tecnologías de la información y la comunicación (TICs). El libro se puede descargar en http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf

ALGUNAS ESTADÍSTICAS DE LOS SERVICIOS PARA LAS REDES SOCIALES[121]

- Al ser preguntados los jóvenes de hasta 30 años por la razón de su entrada en una red, la respuesta en el 95% de los casos fue "porque me invitaron".
- Facebook mantiene activos cada día el 50% de sus usuarios registrados –más de 500 millones. Esto significaría por lo menos 175 millones de usuarios cada 24 horas ... Un aumento considerable con respecto al año anterior
- Twitter tiene ahora 140 millones de cuentas de usuario, pero sólo unos 25 millones son usuarios activos de forma regular. Tiene un crecimiento promedio mensual del 26 por ciento.
- LinkedIn aumenta alrededor de 1 millón de miembros de mes a mes desde julio / agosto del año pasado.
- Flickr ahora alberga a más de 4 mil millones de imágenes. Esto es más de 5 millones a finales de julio de 2009.
- Wikipedia tiene actualmente más de 14 millones de artículos, lo que significa que unos 85 mil colaboradores han escrito casi un millón de nuevos post en seis meses.
- Las fotos en Facebook se han incrementado en más del 100%. En la actualidad, hay alrededor de 2,5 mil millones de fotos subidas al sitio cada mes.
- Hay más de 70 idiomas disponibles en Facebook.
- En el 2009, el promedio de usuarios tenía 120 amigos en Facebook. Esto es ahora alrededor de 130.
- El uso del teléfono celular para participar en Facebook ha aumentado considerablemente. Tiene más de 65 millones usuarios que acceden al sitio a través de dispositivos móviles. En seis meses, esto es más de 100% de aumento.
- Hay más de 3.5 billones de piezas de contenido (enlaces a las webs, noticias, blogs, etc) cada semana para compartir en Facebook.
- El 15% de los blogueros gastan 10 ó más horas cada semana en sus los blogs, según Technorati.
- Twitter procesó casi 10 mil millones de tweets en un solo año.
- Alrededor del 70% de los usuarios de Facebook se encuentran fuera de los EE.UU. Facebook desplazó a Google en la preferencia de los usuarios norteamericanos.
- La India es actualmente el país de más rápido crecimiento para usar LinkedIn, con alrededor de 3 millones usuarios en total.
- Más de 250 aplicaciones de Facebook tienen más de un millón de usuarios combinada de cada mes.
- Hasta un 5% de los candidatos en una entrevista de trabajo son rechazados por sus perfiles en estas redes sociales, a veces inmaduros, con direcciones de correo con nombres infantiles o groseros, de dudoso gusto, y con fotografías inadecuadas o costumbres o grupos de amistad poco recomendables.
- El usuario medio de Facebook tiene entre 20 y 35 años, vive en una ciudad de más de 200.000 habitantes y es de clase alta.

[121] Estadísticas de enero de 2010, tomadas de E-Consultancy. En http://econsultancy.com/uk/blog/5324-20+-mind-blowing-social-media-statistics-revisited



OPORTUNIDADES DE ESTOS ESPACIOS

- Son nichos en los que, sumados, están cautivos entre un 80 y un 90 por ciento de los usuarios de la Internet, es decir más de 1 500 millones de ciudadanos. Por tanto, una oportunidad única para ejercer influencia sobre ese universo. Se espera que en el 2020, estarán conectados a Internet más de 5 000 millones de personas; la mitad de la población mundial, en el 2015, según la Unión Internacional de Telecomunicaciones.
- En un entorno global donde la información es un recurso decisivo en la lucha política, se convierte en un asunto de Seguridad Nacional lograr ventajas competitivas en estos espacios para dar visibilidad y credibilidad a nuestros puntos de vista y nuestros valores. Es imposible construir alternativa desde la marginación, la paranoia y la ignorancia.
- Cuando se conoce la lógica de la llamada web 2.0 y sus herramientas, se posible empoderarse de canales privilegiados para la ofensiva informativa, contrarrestar campañas y construir alternativas para la expresión política.
- Ofrecen una oportunidad sin precedentes para la militancia, que puede multiplicar exponencialmente su fuerza política si logra empoderar a las redes orgánicas con las redes tecnológicas, articuladas con los movimientos progresistas que se expresan por Internet.
- Permiten participar de la experiencia de la innovación permanente que es una de los ejes centrales de la Internet, algo que ya no está solo en las manos de los informáticos o los especialistas.
- Acortan el camino en la búsqueda de información, personas o grupos afines.
- Facilita el contacto con amigos y conocidos de forma rápida e intuitiva.

- Es de fácil manejo, son asequibles sus condiciones de ingreso y resulta gratuito casi siempre.
- Integra recursos a través de enlaces o herramientas de muchos servicios sociales: Youtube, Google, Wikipedia, Blogger, etc…
- Sirven para casi todo: chatear, enviar mensajes a través correo electrónico, bajar y subir música, manejar videos, recopilar información…
- Tiene una protección contra Spam y contenidos indeseados, bastante razonable, y una privacidad relativamente fiable, si se conoce el manejo básico.

RIESGOS

- Pérdida de la privacidad, variable con la que hay que saber lidiar en la Era de la Información. No hay manera de eludirla, salvo aislándonos de la red, lo que equivale al suicido político, económico y social.
- La mayoría de estas plataformas han sido desarrolladas en EEUU, por lo que el gobierno norteamericano tiene acceso a las bases de datos, acción protegida legislativamente.
- Todos los servicios de espionaje del mundo "viven" en las redes sociales, particularmente en las más populares.
- En la mayoría de estos espacios, la retirada supone una maraña de trámites difíciles e incómodos. Siempre quedan trazas.
- Estas redes padecen de hipermnesia, síndrome que provoca el recuerdo autobiográfico perfecto. Es decir, la capacidad de retener cada detalle de una vida, los buenos, los malos, los errores, los aciertos… Un lastre que puede comprometer el futuro de las personas.
- Son de dudosa intimidad, aunque las promociones de muchas de estas redes sociales lo aseguren. El 50% de los adultos mantiene su perfil -datos personales y fotografía básicamente- como de acceso público.
- En muchas ocasiones es un sistema pernicioso y de dudosas verdades, o sirve de plataforma o soporte de algunas lacras sociales.
- Soporta una utilización indiscriminada por parte de los menores, sin filtros internos ni dispositivos de control.
- Camina entre un dudoso control legal por su constante flexibilidad y rapidez evolutiva.
- Lo que hoy es actual mañana es primitivo: sigue la moda de forma brutal, inmediata y despiadada (el 70% de los usuarios tiene menos de 2 años de experiencia en su manejo)
- Genera adicción y puede convertirse en un sustituto adulterado de la vida real.
- Crea el "síndrome de la ubicuidad", consistente en la pertenencia a varias redes sociales y con múltiples contactos, imposibles de mantener o compatibilizar con una vida normal.
- No siempre cualquier tiempo pasado fue mejor: es relativamente frecuente descubrir fallecimientos o desgracias de personas de las que desconocíamos su paradero en algunos tramos de edad y en otras ocasiones, si el encuentro se produce, la amistad después de tantos años es forzada y difícil de mantener. Se pierde en poco tiempo el interés por no existir contacto directo, real. Fomenta amistades superficiales, casi ficticias.
- Es refugio de apuestas diversas encubiertas y enlaces de contenido erótico si su manejo es deficiente o inocente. Hay que detectar y acotar las zonas de riesgo.

ALGUNOS ELEMENTOS DE LA POLÍTICA TODAVÍA EN ANÁLISIS PARA LA PARTICIPACIÓN DE LOS CUBANOS EN ESTOS ESPACIOS

Frente al desafío de las redes sociales en Internet que convierte a los individuos en medios de comunicación y al intento del gobierno de los Estados Unidos de imponer en estos espacios una visión manipuladora de la realidad cubana, es imprescindible estimular la presencia de los revolucionarios en la Web, con vivencias personales, opiniones y acciones que impidan que el enemigo usurpe la expresión de la Isla en un ámbito en el que se informa y expresan millones de personas hoy en el mundo.

Se ha propuesto algunos lineamientos par el acceso a las Redes Sociales

1. El acceso desde el sector institucional estará en dependencia de las oportunidades que ofrecen las Redes Sociales para cumplir su objeto social.
2. La dirección de los Organismos de la Administración Central del Estado, Instituciones, Organizaciones de Masas y las Asociaciones de la Sociedad Civil Socialista Cubana definirán los puestos de trabajo que, por la función que cumplen y los intereses estratégicos del país, deben tener acceso a los servicios de las Redes Sociales.
3. Cada Organismo deberá elaborar sus Normas Generales para regular el acceso a las Redes Sociales en función del interés institucional y del país.
4. Priorizar la presencia en las Redes Sociales de las Instituciones de la Prensa, Cultura, Educación Superior, Instituto Cubano de Radio y Televisión, Relaciones Exteriores, ICAP, Salud, Joven Club, la UJC y las organizaciones de masas y otros que se consideren estratégicos para la batalla en el campo ideológico. En estos organismos, se facilitará el acceso también desde Salas de Navegación Colectiva, puestos de trabajo o a través de cuentas personales de acceso a Internet.
5. Será necesario crear, en un plazo breve, un servicio Web de correo electrónico (Web mail) nacional, público y gratuito con salida internacional, para facilitar el acceso a las Redes Sociales desde nuestro país, sin tener que acudir a servidores ubicados en otros países.

Sobre el Perfil de usuario

1. Cada individuo es una fuente informativa y no hay restricciones para ofrecer información, salvo lo establecido por el Decreto-Ley 199 sobre la protección a la información oficial y el Código Penal vigente.
2. Cada individuo es responsable de todo lo que divulga en la Red, de la misma forma que lo es cualquiera en cualquier otro lugar y está sujeto a las normas de las organizaciones o instituciones a las que pertenece y a lo establecido en el Código Penal.
3. Cada usuario de la red social deberá tener en cuenta la diferencia entre el perfil institucional e individual en las Redes Sociales.
4. El perfil institucional está orientado a los objetivos y características de la institución que vierte información en la Red Social, y el perfil personal, es la opinión individual de una persona.
5. Las instituciones, organismos, organizaciones de masas y asociaciones que empleen las Redes Sociales deberán elaborar su perfil para ese fin.
6. El perfil personal de los líderes de opinión y de las personalidades de los diferentes sectores,

identificados con un medio o institución, es también institucional.

La seguridad de las tecnologías y la Información

1. Mientras persista la agresión mediática del imperialismo y el peligro real de una agresión militar contra Cuba, utilizando pretextos como un éxodo masivo, elevados niveles de indisciplina social, una supuesta violación masiva y flagrante de los derechos humanos, situación de desastre, u otros pretextos parecidos, los usuarios de las Redes Sociales estarán en la obligación de denunciarlo y cuidar que sus opiniones o contenidos no sean utilizados para alimentar dichas campañas o infligir daños al país.
2. De igual forma mientras persista la guerra económica de Estados Unidos contra Cuba los usuarios de las redes sociales deberán tenerlo presente y evitar dar cualquier información considerada clasificada o limitada, que facilite el trabajo a las agencias del gobierno norteamericano dedicadas por más de 50 años a perseguir y sancionar a las empresas que comercian con Cuba, por ejemplo, no se debe informar sobre los suministradores de recursos financieros, materias primas, marcas y patentes en uso.
3. No se debe publicar el nombre, la voz o la imagen de una persona para fines publicitarios, comerciales o de naturaleza análoga. Ni emitir ni promover en estas Redes juicios de valor, u otros contenidos, en ninguno de los soportes: texto, videos, audios, que de cualquier modo denigren, lesionen la dignidad de las persona o de las instituciones.
4. En ningún caso se deben emitir insultos, mensajes racistas, sexistas, que fomenten la violencia ni similar, ni ningún otro contrario a las leyes. También estarán restringidos los mensajes que contengan spam (correo no deseado, cartas cadenas u otros contenidos que se envían masivamente a muchos usuarios que no lo han solicitado).
5. No se puede hacer uso de la Red para transmitir información de carácter comercial o cualquier otra forma que represente un lucro para la persona que lo origina, o la procura, excepto en caso de que haya un interés explícito de las instituciones del país en proyectos de este tipo.
6. Todos los usuarios de la red social deberán cumplir las regulaciones y normas establecidas por el Ministerio de la Informática y las Comunicaciones y en el Decreto ley 199; y tener en cuenta que las computadoras que procesen, reproduzcan y/o almacenen información clasificada, no pueden estar conectadas a redes de alcance global.

VIII- Apuntes sobre la red de información y comunicación del Sistema Nacional de Salud de Cuba: Infomed

Surgimiento y evolución.

Infomed surgió a principios de la década de 1990, justo cuando se inició el período especial. A pesar de la prioridad política que la revolución cubana continuó dando a la salud de la población, el sistema de salud sufrió directamente los embates de la crisis. Todas sus actividades se vieron afectadas y entre ellas las de información científica y técnica que respaldaban el desarrollo del sistema. En ese difícil contexto surgió el Proyecto Infomed con la intención de enfrentar la crisis mediante un cambio estratégico en cuanto a cómo garantizar el respaldo de la información científica y técnica que necesitaba el sistema de salud. Este proyecto le dio un lugar central al desarrollo de capacidades de los recursos humanos y al uso adecuado de las tecnologías de la información y las comunicaciones. Es decir, la crisis se enfrentó con una perspectiva de desarrollo.

Los años del período especial vieron transitar al sistema de información científico-técnica en salud, desde una situación en que predominaban los soportes impresos y se invertían grandes recursos en la importación de literatura, al predominio del uso de servicios y fuentes de información por medios electrónicos.

La red tiene hoy alcance nacional e internacional, sirve a decenas de miles de usuarios regulares y su Portal se ubica entre los primeros sitios Web cubanos y entre los 50 000 portales más visitados entre todos los sitios de Internet. A finales del año 2009 existían 66 852 usuarios registrados en Infomed según cifras del registro de servicios de la red. De ese total de cuentas 49 464 disponían del servicio de acceso conmutado, es decir, suponían una conexión física mediante modem a los servicios de la red. Esta cifra, no considera los usuarios que desde alguna de las redes que conforman el dominio “sld.cu” cuentan con servicios locales de correo electrónico y que operan a través del servicio de Infomed lo cual eleva el número total de usuarios.

Hoy día, todas las revistas cubanas e internacionales en ciencias de la salud y los principales libros de autores nacionales están disponibles a texto completo y en línea para su acceso directo a través de la red Infomed y se cuenta con acceso a los recursos de información en salud más importantes en Internet. Los usuarios de la red tienen acceso a prácticamente todas las revistas científicas que se publican en el mundo así como a bases de datos especializadas y un amplio universo de recursos de información de calidad. A los servicios de navegación se adiciona la extensión, entre los profesionales y técnicos de la salud, del uso del correo electrónico y otras formas de intercambio y colaboración incluidas las consultas con expertos, los cursos virtuales y otras.

Infomed es el resultado de la continuidad del proceso de conformación de un sistema nacional de información científica en salud, que se comenzó a construir a partir de 1965 cuando se fundó el Centro Nacional de Información de Ciencias Médicas. Esta célula inicial se multiplicó en una red de centros provinciales de información que comenzaron a crearse a partir de finales de la década del 1960, hasta cubrir la totalidad de las provincias y el Municipio Especial de la Isla de la Juventud. Es parte de una estrategia en que se han buscado respuestas a las necesidades cambiantes del desarrollo del sistema de salud y a las condiciones en que este ha tenido que funcionar. Es decir, que las intenciones y las metas se han visto determinadas y retroalimentadas por las condiciones concretas de la existencia pero, al propio tiempo, ha habido una acción

intencional y consciente para enfrentar esos problemas y transformarlos en la dirección de dichas metas.

En una primera etapa, la red Infomed creció fundamentalmente al conectar a los Centros de Educación Médica Superior del país y un grupo reducido de instituciones nacionales que contaban con la infraestructura básica para conectarse a la misma. Los Centros de Educación Médica Superior (CEMS) fueron las primeras instituciones que se conectaron (Institutos Superiores de Ciencias Médicas de La Habana, Villa Clara, Camagüey Santiago de Cuba y las Facultades de Medicina de todas las provincias). El proyecto incorporó a los centros provinciales de información de ciencias médicas que formaban la red nacional de información científica y técnica del MINSAP coordinada por el Centro Nacional de Información de Ciencias Médicas (CNICM). Se incluyó la creación de redes locales en todas los CEMS mencionados y equipamiento informático básico para ofrecer servicios de correo electrónico y diseminación de información por esta vía creándose un nodo de Infomed en cada provincia (con la excepción de la provincia Habana). A estas instituciones se adicionó un grupo de centros del MINSAP vinculados con el desarrollo del Polo científico relacionadas con actividades regulatorias. La red se fue expandiendo en la medida que nuevas instituciones de salud fueron contando con los recursos para adquirir el equipamiento que les permitiera conectarse a Infomed.

El Portal de Salud de Infomed comenzó a desarrollarse a partir de1994 con el objetivo de facilitar el acceso a la información relacionada con las ciencias de la salud y especialmente dar acceso a la información de salud producida en Cuba y cuenta para ello con la Biblioteca Virtual de Salud y la Universidad Virtual de la Salud.

Ilustración 1- Imagen de la página principal del Portal de Infomed

El Portal integra además una red de portales especializados que se desarrollan con la participación de las sociedades científicas, grupos nacionales de especialidades y la red de instituciones de salud. El Portal es accesible en la dirección http://www.sld.cu/. Desde su surgimiento la red Infomed formalizó el dominio *sld.cu* que agrupa al conjunto de sitios y servicios de la salud y para el cual está vigente desde 1999 la Política para la publicación en el Web de Salud.

Aspectos institucionales

El Centro Nacional de Información de Ciencias Médicas, fundado en 1965, es la institución del Ministerio de Salud Pública de Cuba que coordina el sistema de información científica y técnica del Sistema Nacional de Salud y la red Infomed.

El Centro Nacional de Información de Ciencias Médicas tiene en su encargo social las siguientes funciones principales:

- Normar y controlar metodológicamente las actividades de información científica y técnica dentro del Sistema Nacional de Salud.
- Brindar servicios de información científica y técnica al Sistema Nacional de Salud para respaldar sus estrategias y programas.
- Coordinar y desarrollar la red de unidades de información científica y técnica al servicio de la salud. Para ello se apoya en los Centros Provinciales de Información de Ciencias Médicas, los Centros Municipales de Información, los Centros Especializados de Información y las Bibliotecas de las unidades del sistema de salud. También trabaja sistemáticamente con sociedades científicas, grupos nacionales de especialidades y otras instituciones nacionales e internacionales para respaldar el cumplimiento de su misión.
- Desarrollar la Biblioteca Virtual de Salud de Cuba para lo cual es centro de referencia nacional y Centro colaborador de la Organización Mundial de la Salud para ese objetivo, y participar en el desarrollo de la Universidad Virtual de la Salud.
- Desarrollar la red Infomed como infraestructura de redes que sustente los servicios de información y de comunicación del sistema de salud y operar como proveedor de servicios de Internet para el sistema.
- Brindar servicios de edición científica de libros y revistas en el campo de las ciencias médicas y de la salud, y promover el desarrollo del sistema de publicación científica en salud.
- Desarrollar programas de formación de los recursos humanos en temas de información científica y técnica y de las tecnologías de la información y las comunicaciones que los sustentan y desarrollar investigaciones que respalden el desarrollo del sistema de información científica y técnica en salud y sus servicios.

La Visión por la que trabaja Infomed hasta el año 2015 es:

Se ha consolidado un sistema de información y conocimientos al servicio de la salud cubana, sustentado en las capacidades de una red de personas e instituciones, que construyen y aprenden de forma cooperada para producir, acceder y usar eficientemente fuentes, servicios y productos de información de alta calidad.

La Misión

Infomed es la red de personas e instituciones cubanas que trabajan cooperadamente en el desarrollo de las capacidades para producir, adquirir, organizar y facilitar el acceso eficiente a la información de calidad que exige la mejora continua de la salud.

Para ello busca:

- Consolidar un sistema de información y conocimientos al servicio de la salud sustentado en una red de instituciones y personas que participan en su construcción y gestión.
- Elevar la calidad de las fuentes, servicios y productos de información y garantizar la universalidad de su acceso.
- Desarrollar espacios de aprendizaje permanente e investigación en gestión de la información y el conocimiento en salud.
- Perfeccionar de manera continua la infraestructura técnica, logística y organizacional y garantizar su uso eficiente y seguro.
- Fortalecer la interacción de la red con otras redes nacionales e internacionales.
- Lograr la sostenibilidad del sistema mediante la movilización de recursos y su uso racional.
- Controlar y evaluar sistemáticamente el funcionamiento del Sistema de acuerdo a sus metas.

Escenarios

- La transformación se realizará en un escenario nacional e internacional político, social y económico complejo.
- Proceso del perfeccionamiento institucional y económico del país y en particular en el sector de la salud, que incluye el reordenamiento laboral.
- Incremento de la escala de servicios para responder a un crecimiento de la demanda.
- La red funcionará crecientemente como una organización virtual.
- La rápida obsolescencia y deterioro del equipamiento afecta la sostenibilidad de la red
- Los recursos materiales dependerán fundamentalmente de la capacidad para movilizarlos.
- Integración creciente con otras redes nacionales e internacionales para lograr el desarrollo.

Valores deseados

- Compromiso consciente y activo de todos los trabajadores con las metas de la revolución y de la Salud Pública cubana.
- Construcción colectiva de la red con la participación activa de sus miembros y el vínculo con la comunidad.
- Cultura organizacional creativa y flexible que responda a las necesidades del sistema nacional de salud dentro de los principios del control interno.
- Actividades basadas en fundamentos científicos y éticos.

- Evaluación permanente como garantía del aprendizaje, el perfeccionamiento y el alineamiento con las metas de la salud.

Áreas de resultados claves

1. Red de unidades de información y personas que trabajan para construir y desarrollar el Sistema de Información en Ciencias de la Salud.
2. Docencia e Investigación.
3. Recursos de Información Científico Técnica al servicio de la salud.
4. Publicación Científica.
5. Infraestructura de sistemas, informática y de comunicaciones.
6. Movilización de recursos.

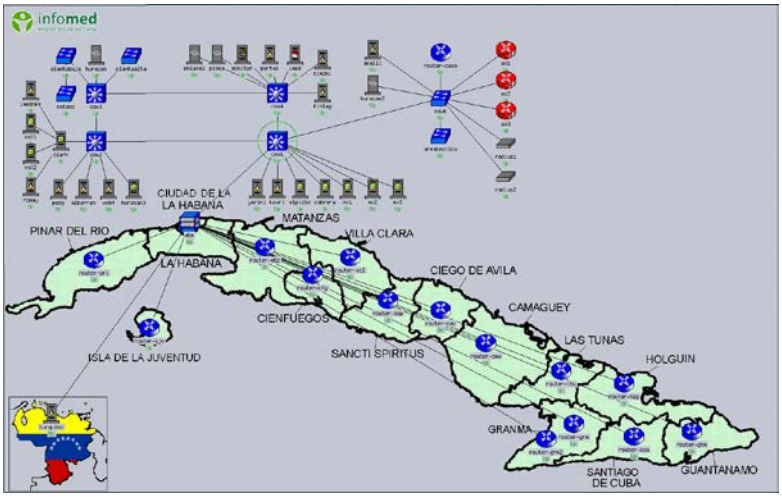
Objetivos estratégicos 2010-2015

1. Consolidar y perfeccionar la red de unidades del Sistema de Información en Ciencias de la Salud.
2. Implantar un sistema integrado de formación continua para los trabajadores del sistema de información basado en competencias.
3. Perfeccionar y desarrollar las metodologías, la infraestructura y los recursos humanos, que respaldan el desarrollo de la Universidad Virtual de Salud.
4. Desarrollar un programa ramal de investigación en ciencias de la información en salud que responda a las necesidades del sistema de salud.
5. Consolidar la Biblioteca Virtual de Salud como el espacio integrado de acceso a los recursos de información en ciencias de la salud dentro del sistema de salud.
6. Elevar la calidad de los procesos de la publicación científica en ciencias de la salud y la visibilidad de la producción científica cubana.
7. Garantizar el acceso eficiente y seguro a los servicios de Infomed del universo de unidades que conforman el SNS para respaldar el cumplimiento de sus misiones.
8. Garantizar los recursos financieros que respaldan la carpeta de proyectos aprobada en función de los objetivos estratégicos.
9. Perfeccionar organizacionalmente el CNICM según estándares de calidad.

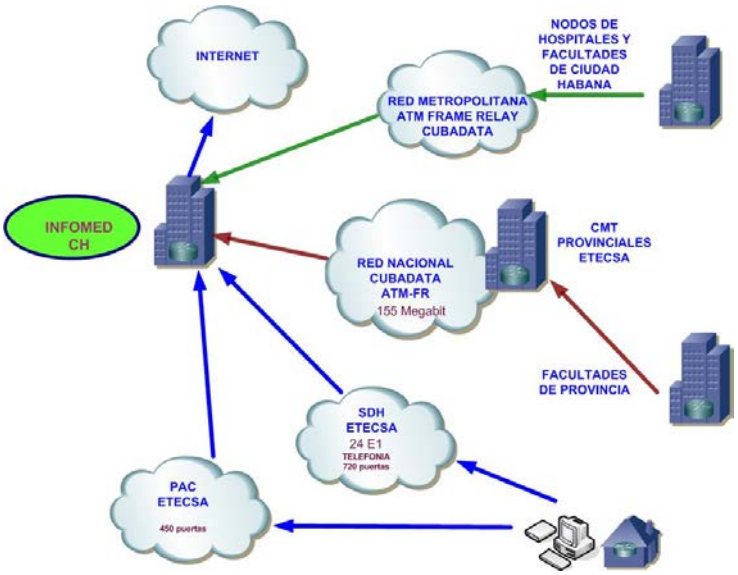
Aspectos técnicos de la infraestructura y los servicios de la red.

Infomed cuenta con un nodo nacional conectado a la red de ATM de ETECSA a 155 Mbit por segundo y 14 nodos provinciales conectados por enlaces de 2 Mbit por segundo y 980 instituciones con enlaces dedicados que oscilan de 64 kbit/seg hasta 2 Mb/seg.

El nodo nacional brinda servicios básicos navegación web, servicios de proxy, servicios de correo, servicios de autenticación telefónica, servicios de FTP, servicios de DNS para toda la red y otros. Además se hospedan servicios de bases de datos y aplicaciones Web que sirven a distintos subsistemas de la salud.



Se mantiene el servicio de hospedaje de páginas Web para las instituciones del Sistema Nacional de Salud y las aplicaciones que soportan los servicios de información de la Red.



Los Nodos provinciales brindan servicios de correo aproximadamente a 6000 usuarios en cada a provincia, servicio de correo a dominios de instituciones de la provincia y 1000 usuarios de acceso telefónico como promedio. Se mantienen servicios de hospedaje de páginas Web para las instituciones de la provincia y las aplicaciones que soportan los servicios de información de los centros provinciales de información. Se mantiene el servicio de enlaces dedicados a las instituciones de la provincia.

Seguridad Informática

La seguridad informática dentro del MINSAP se rige por las regulaciones establecidas al efecto en el país. Cada institución que se conecta a la red debe contar con un plan de seguridad informática y el Ministerio cuenta con un sistema de control de la actividad en correspondencia con su estructura que organiza la dirección nacional de informática. Como parte de la reorganización del MINSAP se está revisando la organización del sistema en la que la dirección de de seguridad y protección asume la actividad de control.

Dentro del Nodo nacional de Infomed ubicado en el Centro Nacional de Información de Ciencias Médicas, existe un departamento de seguridad de la red que realiza el monitoreo de las actividades de la red y cumple actividades de control programado como parte del plan de prevención del centro, que incorpora las actividades del plan de seguridad informática. También atiende de manera sistemática los reportes de incidencias que se generan por las distintas vías. A continuación se exponen una selección de casos que ilustran las actividades de este grupo.

Selección de casos ilustrativos del trabajo para la seguridad de información en la red Infomed.

A continuación se exponen un grupo de casos que ilustran los riesgos, problemas así como el trabajo de la red Infomed en materia de seguridad de información y los resultados de estas acciones.

Caso 1. Uso inadecuado del ancho de banda del canal de Internet

Contexto: La red de Infomed tiene una topología tal que todos los usuarios y instituciones conectados a la red comparten los mismos enlaces (y por ende compiten por el ancho de banda) para acceder a los recursos de Internet. Uno de los servicios más utilizados y que consume mayor ancho de banda es la navegación a Internet. Todas las instituciones conectadas a Infomed tienen acceso a un conjunto de sitios de salud hospedados en Internet y una parte de estas instituciones tienen además acceso pleno a Internet. Para satisfacer la demanda de toda la red nacional de salud se cuenta actualmente con un enlace a 16 Mb/s. Todas las instituciones y usuarios de Infomed que acceden a una página web fuera de la red de salud lo hacen a través de un único servicio proxy administrado centralizadamente.

Hechos: Desde las instituciones con acceso pleno a Internet se navega frecuentemente a sitios no relacionados con contenido de salud y en ocasiones a sitios indebidos según las políticas y la misión de la red. Entre estos últimos están sitios pornográficos, contrarrevolucionarios, de descargas de juegos, música, videos y proxy anónimos.

Causas propiciadoras: A pesar de que existen y se almacenan históricamente las trazas de navegación de toda la red, no existía un sistema de monitoreo y notificación permanente orientado a detectar violaciones en el uso del servicio de navegación a Internet. Tampoco existía un mecanismo de asignación de cuotas de navegación a las instituciones con acceso a navegación en Internet, ni se manejaba el concepto de prioridad en la navegación a ciertos sitios basada en objetivos.

Consecuencias:

- Agotamiento del ancho de banda del canal de Internet.
- Deterioro de la calidad de los servicios de navegación, correo, etc. que hacen uso del canal de Internet.
- Interrupciones recurrentes de los servicios por saturación de estos enlaces.
- Derroche de recursos en actividades ajenas a la misión de la red.
- Violaciones de las regulaciones establecidas sobre el uso de Internet.

Medidas que se tomaron al respecto:

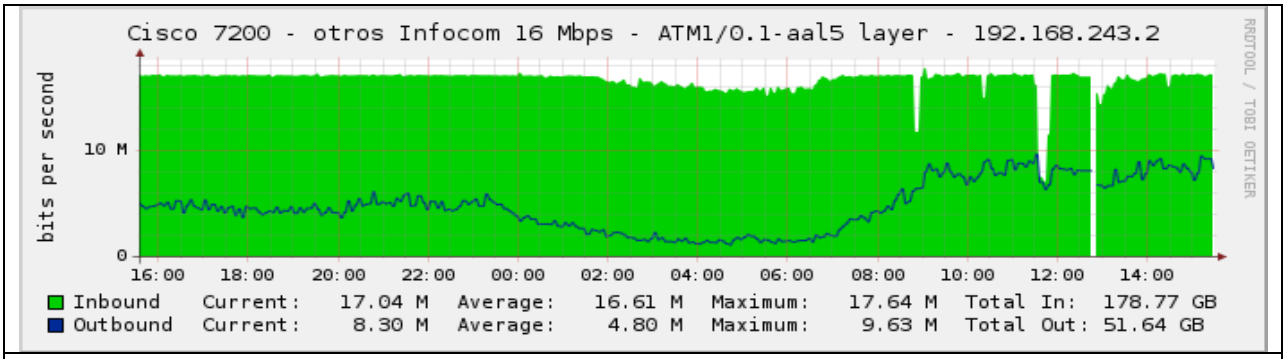
1. Se instrumentó un sistema de chequeo y notificación de violaciones en el uso de la navegación a Internet. Mediante un software desarrollado al efecto se compilan las trazas de navegación cada 24 horas. El sistema permite visualizar la navegación de cada institución organizada por los sitios más visitados. También se filtran las trazas por cadenas de caracteres típicos de sitios pornográficos, de descargas y proxy anónimos. Como resultado del análisis de esas trazas se emite un informe semanal donde se notifican las instituciones donde se cometieron violaciones. Este informe se envía al Departamento de Informática del MINSAP que se encarga de contactar a la institución y monitorear las medidas tomadas. Este informe forma parte de las medidas del plan de prevención de Infomed y se chequea también en la reunión

semanal de los subdirectores.

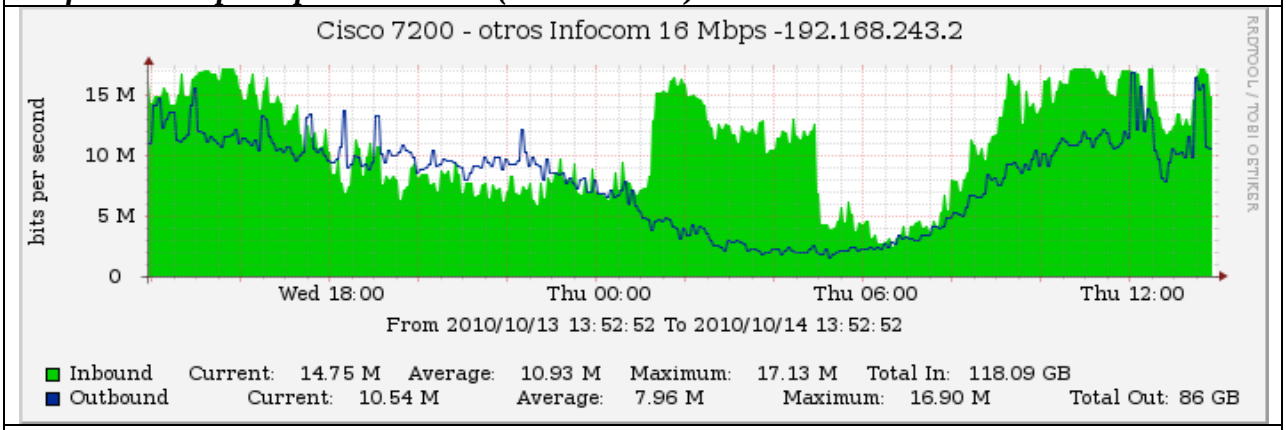
2. Se estableció un sistema de identificación continuo de sitios web esenciales para la salud en función de sus objetivos y programas priorizados a los cuales se les asigna un tratamiento preferencial en cuanto al ancho de banda que permitió elevar la calidad de la navegación a los mismos. Este sistema se basa en el principio de una navegación orientada a objetivos y que responda a la misión institucional.
3. Se implemento un sistema de cuotas de navegación diaria que se aplica a las instituciones con acceso pleno a Internet, que una vez agotada impide la navegación con la excepción de los sitios de salud explícitamente permitidos de acuerdo con el sistema de prioridades mencionado, y los sitios de la intranet nacional(.cu). De tal forma, a pesar de que se agote la cuota de navegación libre, ninguna institución de salud pierde el acceso a los sitios esenciales y al correo electrónico si no se producen violaciones de la política y las regulaciones vigentes.

Resultados:

Se evito la congestión crónica del enlace principal de Internet. Este permanecía saturado durante al menos 18 horas al día y actualmente promedia un 75% de utilización del canal en horario pico. (Ver graficas)



Trafico enlace principal de Internet (Julio de 2009)



Trafico enlace principal de Internet (octubre de 2010)

A partir del momento en que se implemento el chequeo sistemático de la navegación, se comenzaron a identificar las instituciones que incidían sistemáticamente en violaciones, se informo a todas las instancias del MINSAP, se crearon comisiones para investigar, e incluso se tomaron medidas como la suspensión temporal del servicio de Internet a varias instituciones hasta

que se tomaran las medidas que aseguraran el cumplimiento de las políticas y regulaciones establecidas. La sistematicidad de estas acciones, y el aprendizaje por parte de las instituciones ha permitido crear un ambiente de control que ha favorecido la mejoría de la situación. Con el tiempo se ha evidenciado una tendencia a la disminución de estos incidentes y considerando el volumen de la red tanto en número de usuarios como en consumo de ancho de banda los incidentes se mantienen el rango de control. (Ver tabla)[122]

Violaciones detectadas en la navegación a Internet	
Fecha	**Número de incidentes**
4 marzo 2010	7
11 marzo 2010	4
18 marzo 2010	3
26 marzo 2010	4
1 abril 2010	3
8 abril 2010	6
15 abril 2010	5
6 mayo 2010	3
14 mayo 2010	5
20 mayo 2010	4
27 mayo 2010	2
24 junio 2010	1
1 julio 2010	2
9 julio 2010	2
22 julio 2010	1
29 julio 2010	1
6 agosto 2010	2
27 agosto 2010	3
3 septiembre 2010	3
9 septiembre 2010	1
16 septiembre 2010	5
23 septiembre 2010	5
30 septiembre 2010	4

Desde que se estableció el sistema de cuotas y a raíz de las medidas tomadas con instituciones que presentan accesos a sitios que violan las regulaciones, muchas de ellas han reforzado las medidas de control interno y de administración de la cuota disponible, traduciéndose esto en un ambiente de control que comienza a formar parte de la cultura informática de los usuarios. Se ha observado un incremento de la ocupación directa por parte de los más altos directivos del control del tema.[123]

Caso 2. Violaciones asociadas al uso de cuentas de Infomed

Contexto: El servicio de mayor volumen y por tanto de mayor riesgo en cuanto a posibles violaciones son las cuentas de conectividad conmutada a Infomed asignadas a usuarios e instituciones del sistema de salud. Actualmente existen más de 53000 cuentas de conectividad y más de 120 000 cuentas de correo de diferentes tipos (correos de infomed.sld.cu y correos de instituciones dentro del dominio sld.cu).

Causas: En el país existe una gran demanda de servicios de correo electrónico y conectividad que actualmente no se satisface, de ahí que las cuentas de Infomed se convierten en un recurso codiciado y que potencialmente puede ser comercializable ilegalmente. Además esas cuentas pueden ser utilizadas por personas no autorizadas con fines diferentes para los que se han otorgado.

Consecuencias: Se reportan y detectan incidentes relacionados con posibles ventas de cuentas de Infomed, uso por personas no autorizadas y uso indebido de estas.

Medidas que se han tomado al respecto:

1. Fortalecimiento del sistema de monitoreo y control de las cuentas de Infomed y garantía de la trazabilidad del proceso de otorgamiento y uso de las mismas.

[122] El incremento del número de incidentes detectados a partir del 16 de septiembre se debe a que se automatizo la búsqueda de sitios que violan las regulaciones establecidas mediante una lista de cadena de caracteres (ejemplo: porn, xxx, etc.), mejorando la eficiencia en la detección de violaciones. De tal forma se elevó la capacidad de detección de violaciones.

[123] Para resolver este problema no se toman medidas de bloqueo de sitios por URL o por cadenas de caracteres porque la capacidad de procesamiento requerida, el volumen de tráfico, la cantidad de sitios a bloquear y su dinamismo lo hacen inviable en las condiciones de infraestructura de Infomed.

2. Modernización y automatización de la gestión de cuentas de Infomed.-En sus inicios, la gestión (creación y modificación) de cuentas se hacía en la Oficina de Atención a Usuarios de Infomed mediante métodos manuales y usando documentos impresos. De ahí que la trazabilidad del proceso, la detección de violaciones y delimitación de responsabilidades era difícil. Actualmente existe una base de datos de usuarios accesible mediante una interfaz web hecha a la medida de nuestras necesidades y que permite la gestión distribuida de usuarios con varios niveles de privilegios de administración y trazabilidad de cada una de las acciones realizadas sobre las cuentas. Al propio tiempo se mantiene un sistema documentado de delimitación de responsabilidad de las instituciones para la totalidad de las cuentas asignadas que se combina con el sistema automatizado.
3. Chequeo del procedimiento de asignación de cuentas de Infomed- El Departamento de Seguridad Informática realiza inspecciones sistemáticas al proceso de asignación de cuentas de Infomed en el cual están involucrados los directores de instituciones, los representantes designados por ellos y el personal de atención a usuarios. El procedimiento consiste en cotejar la documentación que respalda los cambios en las cuentas coincide con las acciones realizadas en la interfaz de gestión. Esto se hace de manera sistemática (cada 15 días sobre una muestra de 10 instituciones) y ha permitido detectar violaciones y tomar las medidas correctivas. El sistema se ha ido perfeccionado y forma parte del plan de prevención de Infomed chequeándose regularmente en las reuniones de trabajo semanal, reuniones de la comisión de control interno, consejos de dirección y consejos económicos según corresponda.
4. Atención a los reportes de incidentes- Mediante el sistema de reportes (tickets) cualquier persona puede notificar una violación, basta con enviar un correo a la dirección seguridad@infomed.sld.cu dando los detalles del caso. Una vez que se investiga y llega a conclusiones se toman las medidas pertinentes. Estas acciones se realizan de manera coordinada con la dirección de informática del MINSAP y el departamento de seguridad informática.
5. Anclaje de las cuentas de conectividad- El anclaje obstaculiza el robo y la compra-venta de cuentas. Este consiste en la vinculación de las cuentas de acceso a Infomed con un teléfono de manera que no sea posible su utilización desde uno diferente.
6. Publicación en línea para los usuarios con cuenta de Infomed de la lista de usuarios de las instituciones- Esta medida se está implementando. Aunque no se publicaran las direcciones de correo por obvias razones de seguridad, si se podrá ver los nombres de las personas que poseen cuentas en cada institución de manera que a los controles anteriores se adicione el control social de los trabajadores de cada institución de salud, sus directivos y demás organizaciones.

Resultados

El hecho de descentralizar la gestión de usuarios, lo cual implica poner en manos de los directores de instituciones y su representante la autoridad y las herramientas sobre la asignación de cuentas, representa un reto a la seguridad pero es consecuente con el principio de responsabilidad institucional y de control interno. El éxito de esta estrategia radica en el conocimiento por parte del director de la institución y del representante de las responsabilidades que asumen con respecto a la gestión de las cuentas y las implicaciones de cometer una violación. También permite incorporar este proceso dentro de los planes de prevención de cada una de las instituciones y articularlo con el proceso de control interno de cada una de las instituciones. Cada

institución tiene un representante que debe ser seleccionado para representar a la institución antes Infomed y al cual debe controlar por su gestión. Existen además las herramientas para la trazabilidad de sus acciones y las acciones de la institución y cada uno de los usuarios que pueden ser controladas regularmente y permiten la delimitación de la responsabilidad.

Actualmente, aunque se continúan detectando violaciones por parte de directores de instituciones y representantes, se dan como casos aislados. En general se ha incrementado el ambiente de control y la capacidad de detectar las irregularidades. Estas son informadas a las instancias responsables dentro del MINSAP (departamento de seguridad informática, dirección de informática, y Dirección de seguridad y protección), la OSRI además de las instancias administrativas y de control según corresponda.

Caso 3: Problema: Servicios no autorizados desde instituciones conectadas Infomed

Contexto: Las instituciones del MINSAP se conectan a la red Infomed y pueden acceder a todos los servicios de la red, pero no pueden ofrecer ningún servicio hacia la red desde sus redes locales salvo sitios web para publicar información de salud, siempre y cuando haya firmado un contrato previamente con Infomed.

Causas: Frecuentemente los administradores de redes locales colocaban servicios no autorizados disponibles para toda la red de salud, con o sin el consentimiento y conocimiento de la dirección de la institución. Este tipo de acciones se favorece por las propias características de las redes tcp/ip. Entre estos servicios están mensajería instantánea, correo, web mail, ftp, blogs, proxy, accesos telefónicos, etc. Las motivaciones pueden ser muy diversas: lucro, aplicación de conocimientos, entretenimiento, socialización o incluso por desconocimiento colocaban servicios con el fin de desarrollar la red, pero obviando leyes nacionales, reglas de seguridad y estrategias de crecimiento.

Consecuencias:

- Violación de regulaciones sobre seguridad informática.
- Comercialización ilegal de servicios informáticos.
- Degradación de servicios de la red por tráfico excesivo asociado a servicios ilegales.
- Crecimiento caótico de servicios sin tener en cuenta conceptos como sostenibilidad, viabilidad, disponibilidad, calidad, seguridad, etc.
- Acciones de propaganda contrarrevolucionaria y otras violatorias de la seguridad nacional.

Medidas que se tomaron al respecto:

1. Se implementaron reglas de seguridad a nivel de red que impiden acceder a servicios no permitidos. Los puertos de servicios están bloqueados por defecto y se abren solamente para servicios específicos incluidos en los contratos.
2. Se estableció un contrato único entre Infomed y cada institución en el que se explicitan los servicios contratados, sus características y responsables, así como los derechos y deberes de las partes.
3. Se chequea periódicamente el contenido de los servicios web hospedados en las instituciones para verificar que cumpla con las reglas establecidas.

Resultados:

Actualmente es casi mínimo el reporte de incidentes relacionados con servicios ilegales hospedados en las redes de las instituciones dentro del dominio sld.cu. Se han detectado chats, web mails y otros servicios los cuales han sido cerrados tomándose las medidas. Se mantiene el control regular y la toma de medidas de los casos detectados.

Caso 4: Problema: Violaciones cometidas por otras redes nacionales que repercuten en la red de salud

Contexto: Todos los usuarios e instituciones tienen pleno acceso a la intranet nacional. Todas las instituciones y usuarios de Infomed que acceden a una pagina web fuera de la red de salud lo hacen a través de un único servicio proxy administrado centralizadamente por Infomed.

Causas: Como se explico anteriormente, muchos usuarios e instituciones de Infomed, no tienen acceso pleno a Internet, pero si a la intranet nacional. Existen varias formas en que un usuario de Infomed puede usar otra red en Cuba como trampolín para navegar en Internet sin autorización. Básicamente se usa un proxy previamente configurado o se hace un túnel o se usan nombres de dominio .cu que en realidad apuntan a direcciones IP en el exterior. En todos los casos es necesario que en la red utilizada para ello se configure intencionalmente este servicio o como mínimo se dejen vulnerabilidades que propicien la violación.

Consecuencias:

- Navegación no autorizada a Internet.
- Uso de recursos de ancho de banda, proxy, etc. en fines ajenos a los objetivos de la red.
- Lucro

Medidas tomadas al respecto:

1. En los proxys de Infomed se identifica la intranet nacional no por el dominio .cu, sino por los bloques IP asignados a Cuba, antes de tomar esta medida se aprovechaba esta vulnerabilidad para burlar los controles de acceso.
2. Monitoreo periódico de los patrones de tráfico y sitios nacionales más visitados con vistas a detectar comportamientos anormales.
3. Ante cualquier reporte de violaciones de este tipo se reporta inmediatamente a la OSRI y se colabora en esclarecer los detalles de la violación.

Ejemplo:

El día 14 de junio de 2010, se recibe el reporte de que los usuarios de Infomed utilizaban la dirección servermail.vp.co.cu asociada a la IP 200.55.187.242 para navegar en Internet. Se informo debidamente a la OSRI y como resultado de la investigación se identifico a la Escuela Internacional de Medicina Vicente Ponce de Jagüey Grande como origen del incidente. Esta escuela no estaba incluida en el dominio sld.cu pues se conectaba directamente a ENET.

Resultados:

Desde el incidente que se utilizo como ejemplo no se reportan violaciones de este tipo.

IX- Programas malignos y otras amenazas a la Seguridad informática. Acciones para su enfrentamiento

9.1-Definición de Programas Malignos (Malware).

Programas, código ejecutable que realizan acciones no deseadas por el usuario de la PC y que causan daños a la información y/o a los registros y/o programas del sistema operativo y de las Aplicaciones.

Una clasificación elemental podría ser:

Virus: Son programas que se adicionan a otros ejecutables y aprovechan la llamada a estos para replicarse y realizar alguna otra acción maligna con relación a los datos.

Gusanos: No se replican. Se trasmiten aprovechando las vías de comunicación como el correo electrónico. Por lo general son mensajes con anexos que cuando el destinatario le da doble □óld para leerlo o ejecutarlo, se auto envían y realizan otras acciones malignas con relación a los datos.

Caballos de Troya (Troyanos): se solapan a otros programas o aplicaciones, juegos, fotos, películas y al ejecutar la supuesta aplicación se ejecutan y realizan otras acciones malignas.

En la actualidad el malware o los programas malignos se clasifican en:

Backdoor, Constructor, DoS, Email-Flooder, Email-Worm, Exploit, HackTool , Hoax, Macro, Nuker, Packed, Rootkit, Sniffer, SpamTool, SpooferTool y otros (para mayor información sobre estos y otros términos ver el Anexo 10- Glosario sobre programas malignos y otras amenazas).

En el caso de los troyanos tienen una apertura impresionante:

Trojan-AOL, Trojan-ArcBomb, Trojan-Banker, Trojan-Clicker, Trojan-DdoS, Trojan-Downloader, Trojan-Dropper, Trojan-GameThief, Trojan-IM, Trojan-Mailfinder, Trojan-Notifier, Trojan-Proxy, Trojan-PSW, Trojan-PWS, Trojan-Ransom, Trojan-SMS, Trojan-Spy y otros más.

9.2- Antecedentes en Cuba.

El Virus VIENNA.648 fue el primero reportado en Cuba en el año 1988, durante la Convención y Feria Internacional INFORMATICA 88. Se desarrolló una "vacuna" nacional para contrarrestarlo técnicamente. A partir de esta experiencia el Frente de la Electrónica y el INSAC propusieron la creación de un Grupo de Expertos para la Protección de Datos que comenzó el estudio de la problemática y creó una organización para enfrentarla técnicamente.

En 1993 se elaboró y presentó el Proyecto UNESCO: Laboratorio Latinoamericano para la Protección contra los Virus Informáticos con el cual el país recibió un financiamiento para potenciar esta actividad que llegó en 1995 a la creación de la Empresa de Consultoría y Seguridad Informática Segurmática, en el SIME y que pasó al MIC desde su creación cuyo objeto social es el desarrollo de productos y la prestación de servicios de seguridad informática.

9.3- Principales ataques a las redes y aplicaciones informáticas de Seguridad.

Encuestas internacionales del FBI y el CSI (Computer Security Institute) señalan como frecuentes ataques a las Redes de computadoras, los de denegación de servicios, desfiguración de Sitios Web, alteración de sus contenidos, el robo de contraseñas (de tarjetas de crédito, cuentas

bancarias, juegos en línea, acceso a Internet…), las estafas y fraudes financieros que se realizan debido a la insuficiente seguridad de los Sistemas Operativos y Aplicaciones informáticas. Los Programas Malignos se reportan como el principal tipo de ataques a las Redes.

Por esto último existen más de 30 tipos de aplicaciones informáticas para robustecer la seguridad de las computadoras y las Redes, siendo la más utilizada internacionalmente los programas Antivirus.

Adicionalmente se utilizan los Firewalls (Corta fuegos), los IDS (Sistemas de Detección de Intrusiones), los IPS (Sistemas de Prevención de Intrusiones), la Criptografía, las PKI (Infraestructura de Claves Publicas), las VPN (Redes Privadas Virtuales), los programas para el manejo y administración de las vulnerabilidades y los "parches", programas para el análisis de bitácoras y trazas (del Sistema operativo, del uso de Internet y del correo electrónico,…). Existe una gran variedad de estos tipos de aplicaciones informáticas de seguridad, tanto "propietarias" como de código abierto. Segurmática brinda consultoría y realiza proyectos en este tema.

9.4-Principales afectaciones.

Entre las principales amenazas y riesgos se encuentran el Espionaje, extendido a una amplia gama que incluye información militar, gubernamental, económica, industrial, entre otros tipos, mediante el acceso a la información que se envía por los servicios de Internet o que se encuentra en los discos de las redes de computadoras.

- Los ataques a la **disponibilidad** de las TIC. A partir del 2010 la agresión con el virus Stuxnet a Irán, demostró la amenaza que representan para la Seguridad Nacional, los ataques personalizados dirigidos a Sistemas de Infraestructuras críticas. Los autores de estos programas malignos pueden personalizarlos de manera que no afecten a otros países
- La destrucción/alteración de información. Los ataques contra la **integridad** de la información de Páginas Web sin que sus responsables se enteren, inyectándoles textos indeseables que dañan la imagen del sitio y del país que representa y que lo hospeda.
- Computadoras nacionales vulnerables, que sin el conocimiento de sus usuarios y responsables, son incluidas en Botnets (Redes zombis) y desde ellas se mal utiliza la conectividad nacional y hasta se realizan ataques a otras redes por parte de un intruso remoto, aspecto peligroso por el que pueden inculparnos de cometer delitos informáticos y hasta de participar en la Guerra Asimétrica contra los Estados Unidos o alguno de sus aliados.
- La Guerra psicológica y acciones subversivas.

9.5- Comportamiento internacional y nacional actual de los programas malignos.

Internacionalmente los laboratorios antivirus reportan diariamente 30 mil diferentes muestras que implican unas 3 mil a 4 mil firmas diferentes diarias en los antivirus, para poder identificar a todas las muestras diferentes, por lo que se estiman entre 900 mil y un millón de muestras diferentes cada mes, algo prácticamente inmanejable por los antivirus. Con este comportamiento resulta imprescindible mantener el antivirus actualizado. El "mejor" antivirus del mundo, desactualizado, puede crear una FALSA imagen de seguridad y protección, lo cual es peor que no tenerlo. ***Esta es una de las principales vulnerabilidades que se manifiestan en entidades nacionales y que debe ser controlada por los Cuadros que responden por la Informática.***

Según encuestas y publicaciones internacionales, los programas malignos causan anualmente perdidas ascendentes a miles de millones de USD. En los últimos años se han utilizado mucho para realizar estafas y robos lo que hace que el desarrollo de estos, se haya convertido en un negocio muy lucrativo en un mercado subterráneo pagado por una Mafia organizada, aspecto que se corresponde con su incremento exponencial.

Entre algunos ejemplos internacionales de las afectaciones que estos pueden causar, podemos referirnos al intento de robo de 229 Millones de Libras Esterlinas al Sumitomo Mitsui Bank, como un ejemplo de robo con el uso de esta alta tecnología, en el cual se "implantó" un troyano a través de un juego de póker de computadoras.

Como parte de la Guerra económica llevada a cabo por el gobierno de R. Reagan, la CIA organizó una operación para interrumpir los suministros de gas soviético que constituían una importante fuente de ingresos de los países occidentales y que consistió la voladura del gasoducto de la URSS en 1982, por la acción de un caballo de Troya diseñado personalizadamente e introducido de forma solapada como parte del Sistema Informático que controlaba su funcionamiento[124].

En Julio de 2010 se repite este tipo de ataque con el Troyano W32.Stuxnet diseñado para dañar Sistemas SACADA que se utilizan para el control de los llamados Sistemas de Infraestructura Critica (Energía, Telecomunicaciones, Gas, Agua, Tráfico aéreo, y otras unidades industriales …) . En cuanto el Troyano infecta a una de estas computadoras, reprograma el software de los Controladores de Lógica Programables (conocido como PLC por sus siglas en inglés) para dar nuevas instrucciones a las máquinas industriales que controla.

PLC es una computadora "industrial" utilizada para monitorear entradas y dependiendo de su estado toma decisiones sobre la base de su lógica programada. "enciende o apaga equipos, supervisa la temperatura, prende los sistemas de enfriamiento si un indicador muestra una alta temperatura.

Los expertos han especulado que el Troyano podría haber sido dirigido a la planta iraní de energía nuclear de Bushehr o a la planta de enriquecimiento de uranio en Natanz[125].

A partir de ese Troyano bastarían algunos cambios para utilizar el concepto contra otras infraestructuras y objetivos, incluidos los nacionales.

Los Cuadros que atienden las nuevas tecnologías de la Información y en particular la Automática, deben dar al concepto del W32.Stuxnet, el enfoque de Seguridad Nacional que le corresponde.

Principales vías de infección.

– Aprovechando vulnerabilidades de los Sistemas Operativos y de las Aplicaciones.
– Accediendo a sitios inseguros de Internet.
– Abriendo anexos enviados por correo electrónico.

[124] At the Abyss: An Insider's History of the Cold War (ISBN 0-89141-821-0)
[125] http://en.wikipedia.org/wiki/Stuxnet y http://www.symantec.com/content/en/us/enterprise/media/security_ response / whitepapers/w32_stuxnet_dossier.pdf.

– Conectando memorias USB o discos externos.

9.6- Vulnerabilidades de seguridad.

A pesar de la inseguridad de los sistemas operativos y de las aplicaciones de Microsoft, desde hace años se convirtieron en estándares creando una fuerte dependencia a los mismos en los procesos de informatización de todos los países del Mundo, incluyendo al nuestro. Todas las versiones de estos productos de Microsoft han presentado y presentan vulnerabilidades, que aprovechadas por intrusos remotos permiten realizar diferentes tipos de ataques a las redes.

Los ataques van dirigidos a obtener o destruir información, afectar la disponibilidad de las computadoras y hasta controlarlas de forma remota con lo cual realizan espionaje de todo tipo de información, robos de números y contraseñas de tarjetas de crédito y cuentas bancarias así como otros delitos, agresiones y ataques a terceros sin que la mayoría de los "dueños" lo detecten.

Este concepto se extiende de forma general a otras aplicaciones "propietarias" y también a los llamados programas de código abierto, pero estos últimos permiten la posibilidad de que sus usuarios puedan "auditar " el código (tarea bien difícil de realizar), lo que minimiza el problema de inseguridad. Disponer de programas nacionales robustece la seguridad de los Sistemas de infocomunicaciones.

Para solucionar las vulnerabilidades, estas deben ser primero detectadas, publicadas y posteriormente resueltas por sus desarrolladores, para que se pongan disponibles generalmente en el Sitio Web y puedan ser descargadas y ejecutadas en las computadoras para solucionar la vulnerabilidad con el nuevo código que se conoce como "parche". Microsoft todos los segundos martes de cada mes publica un conjunto de "parches" para resolver vulnerabilidades pendientes. También cada cierto periodo de tiempo (un semestre o año) publica los llamados "Service Pack" en los que agrupan un conjunto de "parches" para cada sistema operativo y aplicación que mantiene comercialmente activa.

Este proceso se ha convertido en un concepto imprescindible para los "informáticos" y administradores de redes y no puede ser desconocido por **los cuadros y responsables administrativos que deben exigir su cumplimiento.**

El periodo de tiempo en que una vulnerabilidad es publicada y no se cuenta con un "parche" para solucionarla se conoce como "día cero" y hasta que los usuarios no la solucionen, están sujetos a ser atacados, asumiendo el alto riesgo que esto representa.

El concepto desde el punto de vista de amenaza / riesgo, se incrementa al ser conocido que las agencias de inteligencia enemigas (CIA, NSA…) exigen a los desarrolladores que incluyan "puertas traseras" sin publicarlas de manera que les permitan acceder a través de ellas a la información que se procesa en las computadoras y hasta dominarlas de forma remota.

También son computadoras vulnerables las que por la inexperiencia, incapacidad o negligencia de los administradores de redes, instalan sistemas operativos, aplicaciones o servicios de Internet con las opciones que aparecen por defecto, las cuales en muchos casos no son seguras y dejan brechas para los atacantes.

9.7- Las Redes Zombis o Robots (BotNet):

Las redes zombis o robots, son integradas por computadoras vulnerables (cientos, miles, millones) que un atacante dirige de forma remota desde otro territorio, país o continente para con la fuerza de cálculo de la red, realizar delitos y ataques sin ser descubierto. Una de las aplicaciones de estas redes es la "Guerra Asimétrica" desde donde un tercero puede atacar computadoras de otros países sin ser detectado, ya que los agredidos solo podrán detectar la dirección IP de la ultima computadora que participo en el ataque. Este puede ser un motivo para acusarnos y crear un periodo de Crisis.

Segurmática posee un sistema con el cual captura las direcciones IP (Internet Protocol) de las computadoras nacionales que se encuentren atacando a este, lo cual es síntoma de que un tercero las ha troyanizado sin que sus usuarios y responsables lo noten. En estos casos Segurmática reporta a los Cuadros responsables de cada OACE y de ser necesario brindara los servicios necesarios para solucionar la infección y las vulnerabilidades asociadas.

De forma preventiva Segurmática, a solicitud de los usuarios nacionales, realiza diagnósticos remotos a las redes para detectar posibles vulnerabilidades y solucionarlas antes de que sean aprovechadas por intrusos mal intencionados.

9.8- Algunos aspectos nacionales que los Cuadros deben conocer:

La inmensa mayoría de los antivirus internacionales están plegados a las Leyes del Departamento del Tesoro y de Comercio del Gobierno norteamericano, por lo que explícitamente prohíben su exportación o re exportación a personas naturales o jurídicas de los países considerados en la lista del "embargo", (Bloqueo), o de los países terroristas, en las que Cuba aparece como primero en orden alfabético.

Existen entidades nacionales que por decisión de los administradores de redes, instalan antivirus internacionales con licencias "piratas" con lo que asumen un alto riesgo al utilizar esos antivirus (que no pueden vender sus licencias a Cuba…) y "actualizarlos" desde sitios web .com, ubicados en servidores de otros países. Para estos antivirus no existe la posibilidad de contar con soporte técnico y mucho menos de recibir atención personalizada a la solicitud de incluir en sus bases de firmas la solución técnica ante un nuevo programa maligno hecho intencionalmente para Cuba. Esta situación esulta más dramática ante un ataque vírico intencional que paralice la Red. Estas decisiones corresponden a los Cuadros que responden por la informática y debe tener el correspondiente enfoque de Seguridad Nacional.

Estos no son supuestos y cuando han ocurrido, las respuestas se han realizado con el antivirus nacional de Segurmática y su soporte técnico, el cual se extiende nacionalmente a través de DESOFT.

Hasta la fecha se han reportado más de 100 programas malignos escritos por cubanos o para Cuba. Todos fueron considerados como "día cero" al no encontrar respuesta en los antivirus internacionales y a todos se les dio respuesta técnica con el Segurmática Antivirus

El 27 de Mayo pasado se reporto el primero "polimórfico"(cambia su código cada vez que infecta lo que complejiza su identificación por los antivirus) cuya "muestra" enviamos a los desarrolladores de más de 30 antivirus internacionales y **2 semanas** después, no había respuesta técnica por parte de ellos , por lo que solo el Segurmática antivirus daba respuesta al mismo.

Estos ejemplos sucedidos en tiempo de paz, no pueden ser ignorados por los Cuadros que dirigen la informática nacional. Desde la perspectiva de la Seguridad Nacional, resulta fácil entender lo que sucederá si el enemigo utiliza programas malignos como arma contra las computadoras nacionales. Un programa maligno que se auto envíe solo a direcciones de correo electrónico .cu, podría crear una epidemia nacional sin trasmitirse a otros países, por lo que los antivirus internacionales plegados a las Leyes del Bloqueo, no darían respuesta técnica al mismo. Igual sucedería con programas malignos escritos de forma particular para una entidad nacional.

9.9- Experiencias y servicios de la empresa Segurmática en el enfrentamiento a este problema.

La empresa de Consultoría y Seguridad Informática, mantiene el desarrollo del producto nacional Segurmática Antivirus que ha dado respuesta técnica a todos los programas malignos que se han reportado en el país así como a otros miles internacionales, que de forma preventiva incluye en el antivirus, priorizando los de mayores posibilidades de infectar o de causar mayores daños a las computadoras nacionales. Este desarrollo nacional sería la única respuesta técnica segura ante ataques personalizados contra entidades del país, por lo que resulta muy importante para los directivos que responden por las infocomunicaciones cumplir lo establecido en el **artículo 50 del Reglamento de Seguridad de las TI puesto en vigor por la Resolución 127/07**. Para robustecer la protección antivirus, en aquellos puntos de alto riesgo de la red como los servidores de acceso a Internet y de la mensajería electrónica, en entidades que por su objeto social, tecnologías e intereses del país lo requieran, como complemento del antivirus nacional se instalaran soluciones del motor antivirus internacional de Kaspersky Lab (KL).

Para potenciar este resultado también desarrolla el producto integrado Segurmática Antivirus edición Kaspersky, y distribuye en Cuba soluciones antivirus de ese Laboratorio. Para estas soluciones Segurmatica garantiza un soporte técnico especializado y un servicio de respuesta rápida que se extiende nacionalmente a través de la empresa DESOFT.

Las actualizaciones de los 2 primeros productos se realizan dentro de la red Cuba, desde el Sitio www.segurmatica.cu hospedado en ETECSA. Las actualizaciones de las soluciones de KL requieren acceso internacional al sitio www.kaspersky.com

Teniendo en cuenta la importancia de mantener actualizados los productos antivirus desde tiempo de paz y de disponer de la que de respuesta a un posible ataque personalizado , la actualización del antivirus nacional se encuentra en el Sitio www.segurmatica.cu hospedado en ETECSA así como en otros proveedores de servicios como INFOMED , en las divisiones territoriales de DESOFT y en el Sistema nacional de los JCCE , lo cual resulta un importante apoyo incluso para las entidades que aun no cuentan con la conectividad necesaria para realizar las actualizaciones por la Intranet nacional, las cuales pueden copiar la actualización en una de estas entidades.

La razón social de Segurmática es trabajar por elevar el nivel de seguridad informática de las entidades nacionales para lo cual brinda consultoría y un conjunto de servicios de apoyo a este objetivo. **Entre las principales recomendaciones se encuentran:**

– Copias de Seguridad de los principales datos y programas:

– Que los Cuadros que dirigen la informática exijan y controlen la realización de copias de seguridad actualizadas, de los principales datos generados por las entidades. Para evitar la pérdida de estas se debe almacenar un segundo juego de copias en otro inmueble. Segurmática brinda el servicio de Bóveda de Seguridad.

- **Protección Antivirus:**

Desde el punto de vista de la Seguridad Nacional, resulta imprescindible instalar y mantener actualizado el producto nacional, Segurmática Antivirus. La licencia anual de este producto es respaldada por un soporte técnico especializado.

En entidades de alto riesgo de contaminación vírica, se recomienda tener el antivirus nacional y robustecer las protecciones antivirus con otras soluciones de antivirus internacionales, que se encuentren oficialmente autorizadas y que deben instalarse en los puntos de acceso críticos para la entrada de programas malignos entre los que se identifican el acceso a Internet y a la mensajería electrónica. En las computadoras de la Red local que por su necesidad de intercambio de información a través de soportes externos lo requieran, podrán instalarse los dos motores antivirus activando la protección permanente del nacional y dejando el otro como segunda "opinión" ante casos de duda.

- **Control del uso de los accesos a INTERNET y del correo electrónico:**

Otro aspecto que resulta imprescindible para los Cuadros responsabilizados con la actividad informática en las entidades, es la exigencia del control del uso de los servicios de acceso a Internet y al correo electrónico para que se realicen en función de la actividad social que realizan los autorizados en cada entidad. Las encuestas internacionales consideran en los últimos 5 años que entre el 30 y el 59% de las entidades hacen un mal uso de estos servicios, reportando trabajadores que dedican un alto % de las horas laborales a funciones que no tienen que ver con su trabajo en la entidad y que en muchos casos son acciones delictivas o violaciones del código de ética o reglamentos establecidos.

El control puede realizarse a partir de exigir al administrador de la red el registro de las bitácoras o trazas del uso de estos servicios y su posterior chequeo por los responsables administrativos, para lo cual resulta imprescindible auxiliarse de programas que apoyan esta actividad, como los desarrollados por la empresa de Consultaría y Seguridad Informática u otros existentes de código abierto para los cuales esta empresa brinda soporte técnico y adiestramientos a los encargados de realizar esta función en las entidades.

- **Vulnerabilidades – Parches:**

Realizar Diagnósticos remotos de Seguridad (hackeo ético) a los Servidores de la Red para detectar y solucionar vulnerabilidades antes de que sean aprovechadas por hackers. Este servicio se vincula con el servicio de "parches" y su sistematicidad minimizará las vulnerabilidades.

Además de los servicios expuestos, Segurmática ofrece los siguientes:

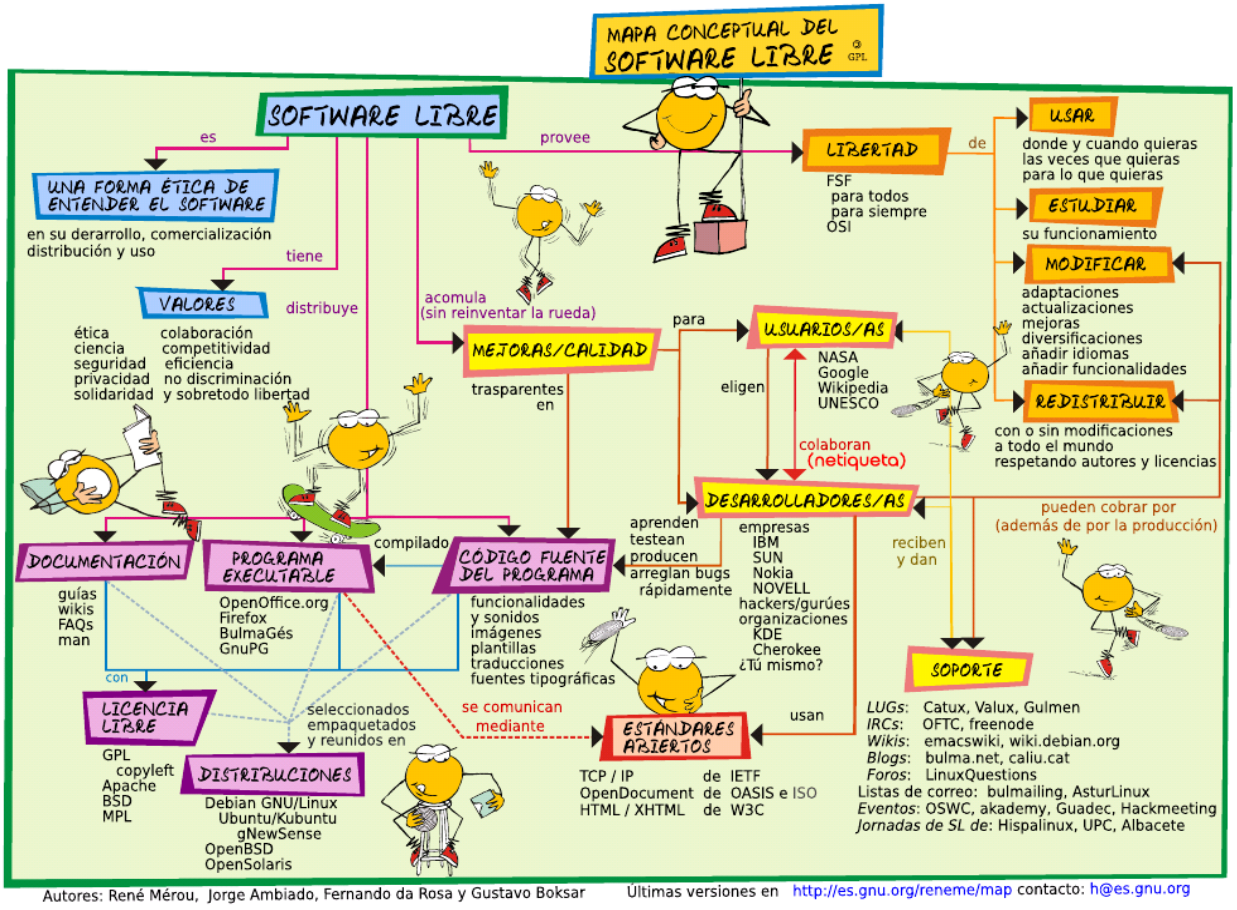
- Elaboración del Plan de Seguridad Informática.
- Realización de dictámenes de seguridad informática.
- Proyectos para asegurar las Redes informáticas.
- Proyectos técnicos para migrar de forma segura a Linux.
- Custodia de material informático. Bóveda.
- Adiestramientos y Consultoría en seguridad informática.

X- Guía cubana para la migración a software libre (extracto)

1-Una introducción necesaria.

Entre los años 60 y 70 del Siglo XX, el software no era considerado un producto sino un añadido, que los vendedores de los grandes computadores de la época aportaban a sus clientes para que estos pudieran usarlos. En dicha cultura, era común que los programadores y desarrolladores de software compartieran libremente sus programas unos con otros. Este comportamiento era particularmente habitual en algunos de los mayores grupos de usuarios de la época. A finales de los años 70, las compañías iniciaron el hábito de imponer restricciones a los usuarios, con el uso de acuerdos de licencia.

Con este antecedente, en 1984 Richard Stallman comenzó a trabajar en el proyecto GNU, y un año más tarde fundó la Free Software Foundation (FSF). Stallman introdujo una definición para free software y el concepto de "copyleft", el cual desarrolló para dar libertad a los usuarios para restringir las posibilidades de apropiación del software.



El Software Libre es aquel que puede ser distribuido, modificado, copiado y usado; por lo tanto, debe venir acompañado del código fuente para hacer efectivas las libertades que lo caracterizan. Es conveniente no confundir el Software Libre con el software gratuito, éste no cuesta nada, hecho que no lo convierte en Software Libre, porque no es una cuestión de precio, sino de

libertad. Algunas personas utilizan los términos "libre" (libre software) y "gratis" (gratis software) para evitar la ambigüedad de la palabra inglesa "free". Sin embargo, estos términos alternativos son usados únicamente dentro del movimiento del Software Libre, aunque están extendiéndose lentamente hacia el resto del mundo. Otros defienden el uso del término open source software (software de código abierto, también llamado de fuentes abiertas).

1.1- Las libertades.

El movimiento del Software Libre hace especial énfasis en los aspectos morales o éticos del software, considerando la excelencia técnica como un producto secundario deseable de su estándar ético. El movimiento Open Source ve la excelencia técnica como el objetivo prioritario, siendo la compartición del código fuente un medio para dicho fin. Por dicho motivo, la Free Software Foundation se distancia tanto de este movimiento.

Software Libre es cualquier programa cuyos usuarios gocen de estas libertades:

- **Libertad 1**: la libertad para ejecutar el programa sea cual sea nuestro propósito.
- **Libertad 2:** la libertad para estudiar el funcionamiento del programa y adaptarlo a las necesidades (el acceso al código fuente es condición indispensable para esto).
- **Libertad 3**: la libertad para redistribuir copias y ayudar al resto.
- **Libertad 4**: la libertad para mejorar el programa y luego publicarlo para el bien de toda la comunidad (el acceso al código fuente es condición indispensable para esto).

GNU/LINUX es un proyecto de más de 20 años en desarrollo, que se asienta sobre una base de cientos de programadores de todas partes del mundo. Es a su vez, el primer sistema operativo basado en UNIX que es 100% Software Libre. Anteriormente había otros sistemas operativos de libre distribución, aunque estos no eran totalmente Software Libre, ya que eran regidos por licencias más restrictivas.

1.2- Las distribuciones.

La base de todo sistema de Software Libre es un núcleo monolítico llamado GNU/LINUX, desarrollado originalmente por Linus B. Torvalds a principios de la década de los noventa. Su estructura general es la típica de cualquier sistema UNIX: núcleo, intérprete de comandos, aplicaciones, procesadores de texto, servidores de red, bases de datos, aplicaciones multimedia y juegos.

El kernel Linux se da en un paquete con un conjunto de programas y aplicaciones de apoyo, procedentes de una serie de empresas como Red Hat, SuSE y Mandrake.

Los contenidos de una distribución deben poder interactuar, y el kernel puede muy bien ser "parcheado" con cambios no disponibles en otras distribuciones. Por ello se puede considerar la elección de una distribución, ya que cada una tiene sus puntos fuertes y débiles.

Hay distribuciones como Debian y Gentoo que no están apoyadas por una empresa comercial y esto tiene ciertas implicaciones por el modo en que se les da apoyo. El apoyo para estas distribuciones procede de terceros y del acceso a listas de correo en Internet. Otras como

Ubuntu, son elaboradas y respaldadas por empresas comerciales y poseen gran aceptación por el usuario final.

1.3- La gran rivalidad.

GNU/LINUX es una familia de sistemas operativos libres y Windows es una de las familias de sistemas operativos privativos, en este caso, propiedad de Microsoft. Si existe un rival para Microsoft Windows casi seguro el más importante es GNU/LINUX, que está ganando cada vez más lugares en el ramo de servidores, por el simple hecho de ser libre, más potente, configurable, seguro y estable.

Aspectos a considerar	Software propietario	Software Libre
Acceso al código fuente	Prohibido por licencia	Si, garantizado
Corrección de errores en el programa por el cliente usuario	No	Si
Duplicación del software	Prohibido	Posible y recomendada
Libertad de competencia para el mantenimiento	No, depende del fabricante	Si, imposible limitarla
Posibilidad de examinar el código del producto	Prohibido salvo permiso del fabricante	Si
Venta de 2da mano	Prohibido	N/A
Respeto a estándares globales	En función del fabricante	En la mayoría de los casos
Adaptaciones al cliente	En función del fabricante	Disponible
Virus, gusanos	Frecuentes	Muy infrecuentes

Algunos autores señalan que para los proveedores del software las ventajas del Software Libre sobre el software propietario van mucho más allá de la parte técnica. Tanto los clientes consumidores de software como sus proveedores mejoran su actividad mediante el uso de Software Libre. Los proveedores pueden ofrecer tiempos de respuesta más bajos, mejor calidad, menos tiempo en Investigación + Desarrollo (I+D), planificaciones más exactas, ahorro en marketing (las aplicaciones libres suelen tener su propia Web, documentación, explicación de ventajas y son de libre descarga y uso), menos pruebas piloto y demostraciones, entre otras. Todo este ahorro se suele invertir en adaptación del software y soporte técnico al cliente.

Es importante señalar que en la mayoría de los casos, las aplicaciones libres reciben contribuciones por parte de las empresas que las usan y así se favorece la mejora global de éstas. Estas contribuciones provienen del uso comercial, de las personalizaciones y de la detección de errores.

Para los usuarios finales (clientes), las ventajas son también numerosas. De las anteriormente mencionadas, las relacionadas con la planificación y el tiempo de respuesta son ventajas para ambos, proveedor y cliente. Por otro lado, el cliente tiene la libertad de probar el software, instalarlo, y, sobre todo, de decidir quién va a ofrecerle el soporte técnico. Este último es un punto clave por el que considerar migrar a Software Libre.

En el caso de Software Libre se puede contar con el respaldo y servicio de diversas distribuciones GNU/LINUX comerciales como RedHat, Suse o Mandriva, las cuales asumen la

responsabilidad de corregir un programa si se presentan fallas, o de emitir los parches o actualizaciones necesarias en el menor tiempo posible. Las actualizaciones pueden ser realizadas por programadores que no pertenecen al equipo original (de desarrollo), de acuerdo a sus intereses y gracias al acceso libre al código fuente.

Algunas distribuciones GNU/LINUX que son completamente libres (como Debian o Ubuntu), ofrecen un adecuado nivel de actualizaciones, sin embargo no existe un compromiso formal con el usuario para este soporte y para el caso de aplicaciones no críticas puede resultar una opción conveniente. Adicionalmente, se abre para el mercado local la posibilidad de ofrecer servicios de soporte y mantenimiento.

Se debe tener en consideración que mientras las actualizaciones que elabora Microsoft son solamente para su sistema operativo Windows, en el caso de las distribuciones GNU/LINUX las actualizaciones abarcan, aparte del sistema operativo Linux, todos los programas que vienen en la distribución, como son: navegadores, paquetes de oficina, programas servidores, aplicaciones multimedia, utilitarios, etcétera; que pueden sumar cientos de programas. Es por ello que no tiene sentido indicar que Windows es más seguro que una distribución GNU/LINUX al tener el primero menor cantidad de actualizaciones.

Otra ventaja para el usuario final o cliente es la existencia de numerosas aplicaciones ya probadas y usadas por cientos o miles de usuarios. Y aún más importante es la posibilidad de descargarlas y usarlas, sin 30 días de prueba ni "banners" publicitarios, simplemente: descargar, instalar y usar.

1.4- Panorama Mundial.

Emitir una opinión sobre el uso de Software Libre requiere de una reflexión sobre diversos temas incluyendo el análisis técnico-económico, pues el Software Libre es considerado un movimiento social cuyo mayor impacto está en las tecnologías de información y comunicación, y a través de ellas en la sociedad en su conjunto.

Una vez que un producto de Software Libre ha empezado a circular, rápidamente está disponible a un costo muy bajo o sin costo alguno. Al mismo tiempo, su utilidad no decrece. Esto significa que el Software Libre se puede caracterizar como un bien público en lugar de un bien privado.

Puesto que el Software Libre permite el libre uso, modificación y redistribución, a menudo encuentra un hogar en los países del tercer mundo para los cuales el costo del software no libre es a veces prohibitivo. También es sencillo modificarlo localmente, lo que permite que sean posibles las traducciones a idiomas que no son necesariamente rentables comercialmente.

La mayoría del Software Libre se produce por equipos internacionales que cooperan a través de la libre asociación. Los equipos están típicamente compuestos por individuos con una amplia variedad de motivaciones.

El Software Libre ha evolucionado y se ha consolidado en muchas partes del mundo teniendo un gran respaldo por parte de académicos, organizaciones educativas, grandes corporaciones, empresas, desarrolladores y usuarios de software. El tema ha trascendido del aspecto técnico para llegar a ser un tema estratégico en muchas organizaciones y un tema político en algunos países. El Software Libre no es una moda, sino es, además de lo indicado, un modelo de negocio para una nueva industria de software basada en servicios, más que en productos.

En muchos países hay antecedentes sobre de migración en entidades gubernamentales

La introducción del Software Libre en entidades del Estado ha ido acompañada de diversos dispositivos o iniciativas legales

La globalización, y en especial la generalización del uso de Internet en el mundo desarrollado han facilitado el advenimiento de operadores globales en el mundo del software. Los mayores, Microsoft, HP, Oracle, IBM, Cisco, son corporaciones transnacionales de origen estadounidense.

El Software Libre se constituye en una alternativa a las soluciones propietarias para la mayoría de los ámbitos públicos y privados. Este conjunto de soluciones informáticas generadas bajo distintas licencias, facilitan la reutilización de la experiencia (al estilo del conocimiento científico) y su uso generalizado y gratuito.

Actualmente existen numerosos programas distribuidos de manera libre ejecutándose en miles de máquinas. El auge de Internet ha favorecido claramente su extensión, al ser distribuidos de manera sencilla. Los programas, creados por personas altruistas y de manera desinteresada, son utilizados ya por miles de empresas y personas. Estas últimas se agrupan en comunidades con intereses comunes.

1.5- Cuba

Ningún país soberano debería estar sujeto a las reglas de marketing de una empresa de software que basa su éxito en el mantenimiento de una situación de monopolio. Ningún Estado debería estar sometido tecnológicamente a otro y más cuando es un país bloqueado económicamente por el gobierno de los EEUU. El software libre contribuye a la igualdad entre los pueblos al permitir el libre acceso de todos a la Sociedad del Conocimiento.

Si una empresa u organismo de un país basa su informatización en software “cerrado” (aquel cuyo código fuente le es desconocido), ¿qué garantías tiene de que los programas hagan únicamente lo que se espera de ellos? ¿Cómo tener la seguridad de que no hay procesos ocultos o defectos que menoscaben la privacidad de la información? Y si son computadoras conectadas a Internet, ¿no es aún más arriesgado no saber como funciona el programa de correo ó el navegador web, por ejemplo?

Para los países en vía de desarrollo es una limitante el excesivo costo de las licencias de los sistemas operativos que suelen utilizar la mayoría de las computadoras (Windows98/NT/2000/XP). Además, está el precio de las licencias de los programas específicos (MS Office, Corel-Draw, Adobe Photoshop, SAP, etc). También hay que tener en cuenta que cada licencia sólo puede ser utilizada en una única computadora. El precio final del software está, por tanto, en función del número de computadoras de que disponemos. Esta inversión tampoco es para toda la vida, ya que el ciclo de vida del software es muy corto.

Sin duda alguna, el uso del Software Libre es sustentable en Cuba a partir de las ventajas que tiene con respecto a los del tipo privativo. Por esto, su aplicación como plataforma informática de trabajo adquiere una relevante significación que puede verse desde ámbitos diferentes:

POLÍTICO: Desde un primer punto de vista, representa la no utilización de productos informáticos que demanden la autorización de sus propietarios (licencias) para su explotación. Es válido recordar que, en el presente Cuba se encuentra a merced de la empresa norteamericana Microsoft, que tiene la capacidad legal de reclamar a Cuba que no siga utilizando un sistema operativo de su propiedad, basado en leyes de propiedad industrial por las cuales también Cuba se rige, a pesar de que la empresa no desee venderle software a la isla; esto provocaría una interrupción inmediata del programa de informatización de la sociedad que como parte de la

batalla de ideas está desarrollando el país, además pudiera implementarse una campaña de descrédito a la isla, abogando el uso de la piratería informática por parte de las instituciones estatales cubanas.

Desde un segundo punto de vista, el Software Libre representa la alternativa para los países pobres, y es por concepción, propiedad social, si se tiene en cuenta que una vez que comienza a circular rápidamente se encuentra disponible para todos los interesados sin costo alguno o en su defecto a muy bajo costo.

En tercer lugar, es desarrollado de forma colectiva y cooperativa, tanto en su creación como en su desarrollo cuantitativo y cualitativo, mostrando su carácter público y sus objetivos de beneficiar a toda la comunidad.

La posibilidad de usar, copiar, estudiar, modificar y redistribuir libremente el software como un bien social, que brinda esta plataforma, cumple los preceptos enunciados por la sociedad socialista cubana y está acorde con el tipo de economía socialista, donde el valor social está por encima de la ganancia.

ECONÓMICO: Su utilización no implica gastos adicionales por concepto de cambio de plataforma de software, por cuanto es operable en el mismo soporte de hardware con que cuenta el país.

La adquisición de cualquiera de sus distribuciones puede hacerse de forma gratuita, descargándolas directamente de Internet o en algunos casos a muy bajos precios. Se garantiza su explotación con un mínimo de recursos, por cuanto no hay que pagar absolutamente nada por su utilización (no requiere de licencia de uso, las cuales son generalmente muy caras), distribución y/ o modificación.

El uso del Software Libre desarrollado con Estándares Abiertos, fortalecerá la industria del software nacional, aumentando y fortaleciendo sus capacidades. Facilitará la reducción de la brecha social y tecnológica en el menor tiempo y costo posibles. Su uso en la Institución Pública y en los servicios públicos, facilitará la interoperabilidad de los sistemas de información del Estado, contribuyendo a dar respuestas rápidas y oportunas a los ciudadanos, mejorando la gobernabilidad.

TECNOLÓGICO: Permite su adaptación a los contextos de aplicación, al contar con su código fuente, lo cual garantiza un mayor porciento de efectividad, además de la corrección de sus errores de programación y la obtención de las actualizaciones y las nuevas versiones.

Todas las mejoras que se realicen no tienen restricciones. De este modo, cualquier otra administración, empresa, institución o organismo se puede beneficiar de las mejoras introducidas.

Se fomenta la innovación tecnológica del país. Al disponer del código fuente de la aplicación, se puede realizar el desarrollo de mejoras, en vez de encargarlas a empresas de otros países que trabajan con sistemas de licencia propietaria. De este modo, se contribuye a la formación de profesionales en nuevas tecnologías y al desarrollo local bajo los planes estratégicos del país.

Garantiza un proceso de corrección de errores muy dinámico. Los usuarios del programa de todo del mundo, gracias a que disponen del código fuente del programa, pueden detectar los posibles errores, corregirlos, y contribuir con sus mejoras.

Limita la introducción de código malicioso, espía o de control remoto; debido a que el código es revisado por muchos usuarios que pueden detectar posibles puertas traseras.

Por las razones detalladas anteriormente, el uso del Software Libre es, sin lugar a dudas, sustentable para Cuba. En ese sentido, desde octubre del 2002, se puso en marcha una estrategia para alcanzar la independencia en el terreno del software, garantizando la seguridad informática y, por sobre todas las cosas, afianzando el uso de los principios del Software Libre, pues la negación de dichos preceptos constituiría el rechazo de los principios del socialismo y el comunismo.

En Abril de 2004 el Consejo de Ministros adoptó el Acuerdo 084/2004 donde indicaba al Ministerio de la Informática y las Comunicaciones (MIC) ordenar el proceso paulatino de migración de Cuba a Software Libre. En el año 2005 se crea el Grupo Nacional para la Migración presidido por el Ministro del MIC. Durante el año 2005 y principios del 2006, el país creó y consolidó el Grupo Técnico Nacional de Software Libre, el de capacitación y el legal.

La avanzada para la migración a software libre del país está centrada en organismos tales como:

- Aduana General de la República.
- Universidad de las Ciencias Informáticas (UCI).
- Ministerio de la Informática y las Comunicaciones.
- Ministerio de Educación Superior y algunas de sus universidades (Área de Servidores).
- Ministerio de Cultura.
- Oficina Nacional de Estadísticas.

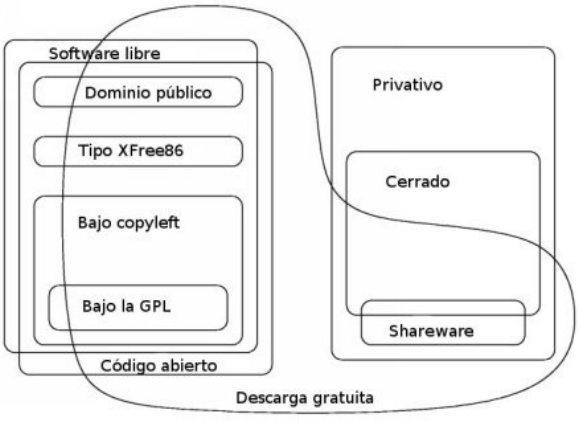
2. CATEGORÍAS y LICENCIAS.

En el mundo del software libre se utilizan a diario programas informáticos, muchos descargables desde internet, que en menor o mayor medida permiten utilizar algunas de sus funcionalidades, en dependencia del tipo de software. Algo similar ocurre con las licencias de estos productos. Estas últimas constituyen la base de los acuerdos entre desarrolladores y usuarios finales para la ejecución y utilización de los programas, de ahí que su dominio se haga absolutamente necesario.

Pretendemos aquí introducir al lector en las diferentes categorías de software existentes hoy en el mundo y realizar un primer acercamiento a los temas de las licencias.

2.1- Categorías de Software.

He aquí un esquema de varias de las categorías de software que se mencionan frecuentemente en discusiones sobre software libre. A continuación se explicarán las principales:



2.1.1- Software de código abierto (open source).

En 1998, una parte de la comunidad decidió dejar de usar el término “free software” (software libre) y usar “open source software” (software de código abierto), con el propósito de evitar la confusión de “free” con “gratis”. Otros, sin embargo, apuntaban a apartar el espíritu de principios que ha motivado el movimiento por el software libre y el proyecto GNU, y para

resultar atractivos a los ejecutivos y usuarios comerciales. Open source se centra en el potencial de realización de software de alta calidad, pero esquiva las ideas de libertad, comunidad y principio.

"Free software" y "open source" describen la misma categoría de software, más o menos, pero reflejan diferentes puntos de vista acerca del software y acerca de los valores. El proyecto GNU continúa utilizando el término "free software" para expresar la idea de la libertad, haciendo especial énfasis en los aspectos morales o éticos del software, considerando la excelencia técnica como un producto secundario deseable de su estándar ético.

2.1.2- Software de dominio público.

El software de dominio público es un tipo de software que no está protegido con copyright. Es un caso especial de software libre no protegido con copyleft, que significa que algunas copias o versiones modificadas no pueden ser libres completamente. "Dominio público" es un término legal y significa de manera precisa "sin copyright".

2.1.3- Software protegido con copyleft.

El software protegido con copyleft es software libre, cuyos términos de distribución no permiten a los redistribuidores agregar ninguna restricción adicional cuando estos redistribuyen o modifican el software. Esto significa que cada copia del software, aún si ha sido modificado, debe ser libre. El proyecto GNU protege mediante copyleft casi todo el software que producen, con el propósito de dar a cada usuario las libertades que el término "software libre" implica. Copyleft es un concepto general. Para proteger actualmente un programa con copyleft se necesita usar un conjunto específico de términos de distribución. Hay muchas maneras posibles de hacerlo.

El copyleft usa la ley de copyright pero le da un giro para servir a lo opuesto de su propósito usual. En lugar de ser un medio de privatizar el software, se transforma en un medio de mantener libre al software. La idea central del copyleft es dar a cualquiera el permiso para correr el programa, copiarlo, modificarlo y redistribuir versiones modificadas, pero no se da permiso para agregar restricciones propias. De esta manera, las libertades cruciales que definen al software libre quedan garantizadas para cualquiera que tenga una copia transformándose en derechos inalienables.

Para que el copyleft sea efectivo, las versiones modificadas deben ser también libres. En caso de de agregarse o combinarse algo a un programa bajo copyleft, debe garantizarse que la versión combinada total sea también libre y bajo copyleft.

La implementación específica de copyleft para la mayoría del software GNU es la Licencia Pública General de GNU (GNU General Public License) o GPL GNU para abreviar. Si bien la licencia GPL ofrece grandes beneficios, en ocasiones ofrece ciertas restricciones. Un ejemplo es que un software que utiliza algún componente GPL, debe sí y solo sí ser licenciado bajo la misma, es decir, no se pueden utilizar partes o bibliotecas de software GPL en un software propietario o distribuido bajo otra licencia.

2.1.4- Software libre no protegido con copyleft.

El software libre no protegido con copyleft viene desde el autor con autorización para redistribuir y modificar así como para añadirle restricciones adicionales. Si un programa es libre pero no protegido con copyleft, entonces algunas copias o versiones modificadas pueden no ser libres

completamente. Una compañía de software puede compilar el programa, con o sin modificaciones, y distribuir el archivo ejecutable como un producto propietario de software.

2.1.5- Software semilibre.

El software semilibre no es libre, pero viene con autorización para usar, copiar, distribuir y modificar (incluyendo la distribución de versiones modificadas) sin fines de lucro. PGP (Pretty Good Privacy) es un ejemplo de un programa semilibre.

El software semilibre es una apuesta un poco más visionaria que el software propietario, pero aún plantea problemas y además no puede usarse en un sistema operativo libre. .

2.1.6- Software propietario.

El término "software propietario"(o privativo) es software que no es libre ni semilibre. Su uso, redistribución o modificación está prohibida, requiere que usted solicite autorización o está tan restringida que no pueda hacerla libre de un modo efectivo.

2.1.7- Freeware.

La palabra "freeware" no tiene una definición clara aceptada, pero es usada comúnmente para paquetes que permiten la redistribución pero no la modificación (y su código fuente no está disponible). Estos paquetes no son software libre.

2.1.8- Shareware.

El vocablo significa literalmente programa compartido e indica que cualquiera pueda descargar el programa y empezar a emplearlo sin desembolso previo durante un período de prueba. Esto no significa que sea de libre uso o de empleo gratuito. La licencia de uso indica con claridad en cada caso los términos de empleo, así como la cantidad que debe ser abonada en caso de encontrarse de utilidad el programa.

El sistema shareware se utiliza a menudo como medio para distribuir versiones de prueba con un costo mínimo. Las versiones de prueba, en general tienen algún tipo de limitación. En algunos casos, algunas funciones no están disponibles; en otros, el programa solo admite una cierta cantidad, reducida de datos. En su versión más popular, el programa tiene toda su funcionalidad, pero solo es operativo durante 30 días tras su instalación. Al cabo de estos, unos programas dejan de funcionar y recuerdan que deben ser desinstalados de la computadora o pagados. Algunos programas simplemente recuerdan cada vez que se ejecutan que el período de prueba ha terminado, pero siguen operativos.

El shareware no es software libre.

2.1.12- Software comercial.

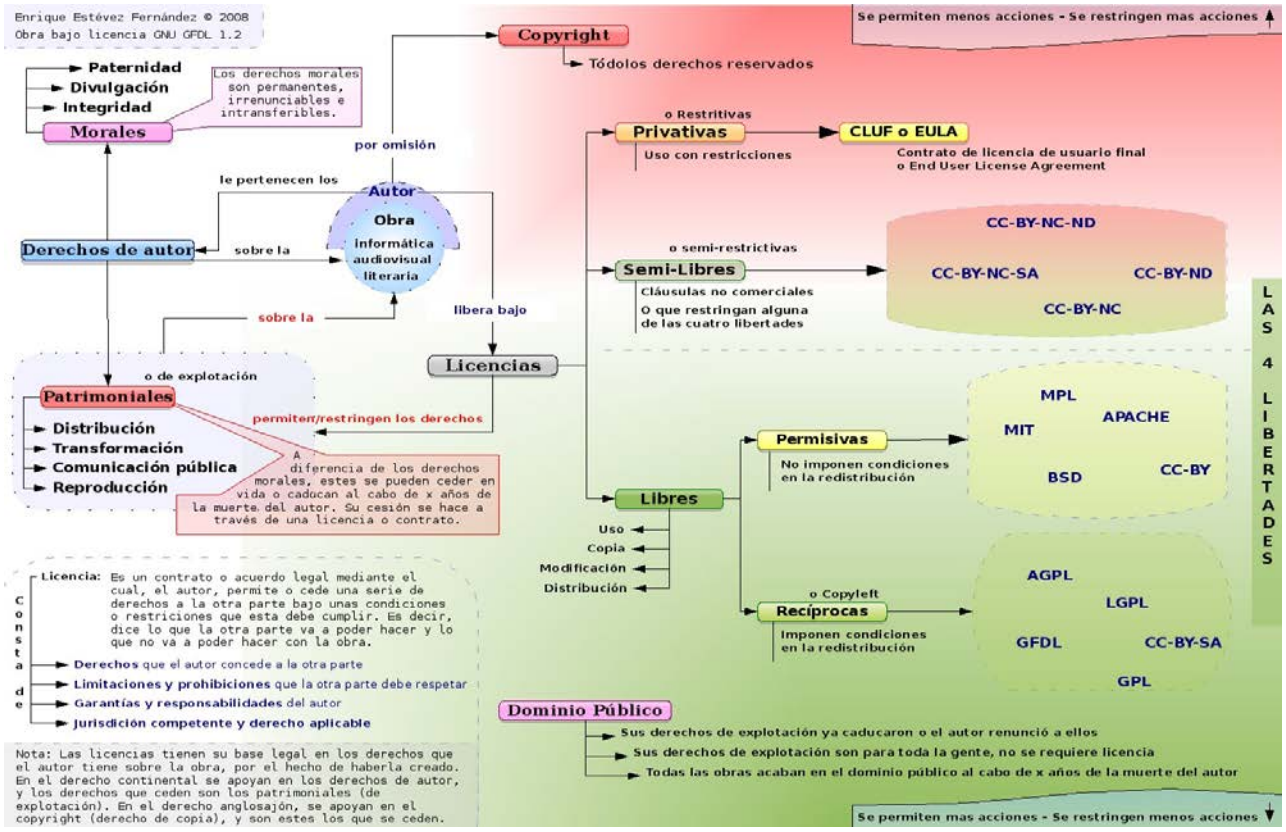
El término "software comercial" se utiliza para el software que está siendo desarrollado por una entidad que tiene la intención de generar ganancias económicas mediante el uso del software. Comercial y propietario no son equivalentes. La mayoría del software comercial es propietario, o sea, es propiedad de una empresa que lo desarrolla con el interés de obtener ganancias por su uso y comercialización. No obstante, hay software libre con intereses comerciales, aunque por lo general el software libre es no comercial.

2.2- Licencias de Software Libre.

Una licencia de software es un contrato entre el titular del derecho de autor (propietario) y el usuario del programa informático (usuario final), para utilizar éste en una forma determinada y de conformidad con unas condiciones convenidas.

Todo software se encuentra bajo una determinada licencia, que poseen características muy diferentes entre ellas, y que si las ignoramos pueden convertirnos en delincuentes. Entender las licencias de software es algo importantísimo para cualquier usuario o cualquier persona o entidad relacionada con la informática, ya que le permite manejarse siempre dentro del marco legal y conocer que existen alternativas que nos dan muchas más libertades que otras.

Las licencias de software pueden establecer entre otras cosas: la cesión de determinados derechos del propietario al usuario final sobre una o varias copias del programa informático, los límites en la responsabilidad por fallos, el plazo de cesión de los derechos, el ámbito geográfico de validez del contrato e incluso pueden establecer determinados compromisos del usuario final hacia el propietario, tales como la no cesión del programa a terceros o la no reinstalación del programa en equipos distintos al que se instaló originalmente.



2.2.1- Software bajo licencia BSD.

Berkeley Software Distribution (BSD). Es la licencia original de una distribución de Software que acabó convirtiéndose en un derivativo de UNIX. Ha tenido dos formas fundamentales: la clásica (con la cláusula de publicidad) y la actual (sin esa cláusula desde julio del 99).

Esta licencia tiene menos restricciones en comparación con otras como la GPL estando muy cercana al dominio público. La licencia BSD al contrario que la GPL permite el uso del código

fuente en software no libre. El autor, bajo esta licencia, mantiene la protección de copyright únicamente para la renuncia de garantía y para requerir la adecuada atribución de la autoría en trabajos derivados, pero permite la libre redistribución y modificación.

2.2.2- Software bajo licencia Apache.

Creada por la Apache Software Foundation (ASF). La licencia Apache requiere la conservación del aviso de copyright y el disclaimer, pero no es una licencia copyleft, ya que permite el uso y distribución del código fuente para software libre y software propietario.

La licencia Apache es una descendiente de las licencias BSD por lo que no es GPL. Esta licencia permite hacer todo tipo de cosas con el código fuente (incluyendo productos propietarios) siempre que se les reconozca su trabajo. Todo el software producido por la ASF o cualquiera de sus proyectos está desarrollado bajo los términos de esta licencia.

La fundación Apache (Apache Foundation) recibe dinero de todas las empresas que venden productos basados en apache (HP, IBM, Oracle, Sun). Con este dinero se paga a los desarrolladores. El producto se regala a la gente...y esas empresas venden sus propias versiones "mejoradas" del producto.

2.2.3- Software bajo licencia Mozilla.

Mozilla Public License (MPL), es una licencia de código abierto y software libre. Fue desarrollada originalmente por Netscape Communications Corporation –una división de la compañía “América Online”, y más tarde su control fue traspasado a la “Fundación Mozilla”.

Cumple con la definición de software de código abierto y con las cuatro libertades del software libre enunciadas por la Free Software Foundation (FSF). Sin embargo la MPL deja abierto el camino a una posible reutilización no libre del software, si el usuario así lo desea, sin restringir la reutilización del código ni el relicenciamiento bajo la misma licencia.

2.2.4- Software bajo licencia GPL 3.

Lo esencial de la GPL no ha cambiado respecto a GPL2: libertad de usar el programa, libertad de estudiar el funcionamiento del programa, y adaptarlo a las necesidades, libertad de distribuir copias, libertad de mejorar el programa y hacer públicas las mejoras.

En esta nueva versión se intentan solucionar una serie de problemas a los que se ha tenido que enfrentar la comunidad del software libre, entre ellos el tema de patentes de software y el conocido como tivolizacion. Con GPLv3, si una empresa utiliza software con esta licencia ofrece permiso gratuito para utilizar las patentes que lo cubren al resto de usuarios. Garantiza además que los acuerdos de protección de patentes como el que hicieron Microsoft y Linspire o Microsoft y Novell se extiendan al resto de usuarios de ese software.

3- Pensando en el futuro.

Hay ciertas circunstancias que pueden hacer que la introducción del software libre sea más fácil.

Muchas de las aplicaciones del software libre funcionarán con sistemas operativos propietarios y esto brinda la oportunidad de introducir estas aplicaciones sin tener que cambiar totalmente el entorno. Por ejemplo, Open Office (Suite Ofimática) y Firefox (Navegador Web) funcionarán con Windows y así pueden utilizarse en sustitución de Office, e Internet Explorer respectivamente. Este enfoque permite que la reacción del usuario pueda ser calibrada a pequeña

escala y que los planes para la formación de los usuarios puedan hacerse sobre la base de la experiencia real. Además, problemas como la conversión de formatos de archivos, macros y plantillas se puede facilitar si la antigua aplicación se mantiene disponible durante algún tiempo.

Muchas guías coinciden en afirmar que los primeros cambios son los que no afecten a la comunidad de usuarios. Eso quiere decir que estos se harán en el servidor, proporcionando la plataforma para la posterior introducción de los cambios en el lado del cliente, que serán compatibles con el entorno actual, con lo que se podrá minimizar el efecto de ruptura.

Por ejemplo, los servidores de nombres DNS, los servidores DHCP y los servidores de bases de datos principales con bases de datos propietarias como Oracle podrían ser todos ellos candidatos a ser reemplazados por herramientas de software libre equivalentes y seguir interactuando con el resto de los sistemas actuales como antes.

3.1- Primeras transformaciones.

Es importante evitar tomar decisiones que puedan dificultar la migración en el futuro. En este sentido es preciso:

1- Insistir en que los desarrollos web hechos tanto internamente como por empresas contratadas para ello, produzcan un contenido que se pueda visualizar en todos los navegadores actuales de la web, en particular los navegadores de software libre. Esta sería una buena práctica en cualquier caso ya que no debería requerirse software específico para visualizar su contenido. Hay herramientas como Weblint y otras más recientes, para comprobar la compatibilidad de las páginas web.

2- No fomentar el uso indiscriminado de macros y scripts en documentos y hojas de cálculo; encontrar otros modos de proporcionar la necesaria funcionalidad. Ésta también es una buena práctica ya que de forma habitual los virus se valen de las macros y los scripts para infectar los sistemas. Además, las macros se pueden usar fácilmente para robar datos y corromper documentos: por ejemplo, podrían hacer que el documento diga cosas diferentes dependiendo de la persona que lo esté leyendo y que se imprima cualquier otra cosa.

3- Insistir en el uso de formatos de archivos abiertos y estándar, como PostScript y PDF.

Se están haciendo intentos para crear formatos de archivos estándar basados en XML y OpenOffice.org es un candidato. Sin embargo, sólo porque un archivo esté basado en XML ello no significa que vaya a ser abierto.

Office Open XML (también llamado OOXML u Open XML) es un formato de documento electrónico creado y desarrollado por Microsoft. Las especificaciones de este formato han sido desarrolladas por Microsoft para suceder a sus formatos binarios de archivo, y cedido a organismos de estandarización como ECMA e ISO. Pero no es abierto, ni es estándar ni es XML

En particular, no se deben usar formatos de archivos propietarios para archivos que son sólo para lectura y que el receptor no los va a editar.

4- Al escribir documentos en colaboración con otros, usar el formato que sea mínimo común denominador. Por ejemplo, hacer uso del formato Word 2003 en lugar de Word 2007. Esto aumentará la posibilidad de que las aplicaciones de software libre puedan participar.

5- Desarrollar sistemas basados en por lo menos un modelo de tres niveles donde el código de

aplicación es independiente de la interfaz humana y de los métodos de acceso a los datos. Por ejemplo, si es posible, tener una interfaz de navegador que se pueda usar en un navegador de software libre. Construir aplicaciones de esta forma modular facilitará hacer la migración bit a bit. Esto no sólo reducirá la escala de cualquier fase de migración sino que también reducirá el riesgo de fallo.

6- Insistir en que las nuevas aplicaciones se escriban de manera que se sean portables. Esto incluye el usar lenguajes estandarizados portables como ANSI C, Java, Python y Perl, y usar sólo librerías multiplataforma y juegos de herramientas GUI. Evitar lenguajes y APIs de arquitecturas específicas. Evitar la construcción de aplicaciones que requieran la presencia de otras aplicaciones propietarias.

7- Apartar a los usuarios de lectores de correo propietarios que usen formatos de buzón propietarios y se comuniquen con servidores que usan protocolos propietarios. La mayoría de las aplicaciones de correo guardarán el correo usando IMAP. Si es posible, hallar el modo de guardar la información del calendario y de la libreta de direcciones en formato abierto.

8- Consultar a todo el personal y que este se mantenga informado de lo que se va haciendo. Un modo de hacerlo es crear una intranet que se pueda mantener actualizada fácilmente y en la que haya una sección dedicada a las opiniones de los usuarios.

3.2- Las reacciones.

Hay ciertas reacciones típicas a los cambios en las prácticas laborales que habrá que afrontar:

El uso del software libre será completamente nuevo para la mayoría de los usuarios y el personal de sistemas. El miedo a lo desconocido hará que las personas se resistan al software libre porque es nuevo para ellas.

Habrá usuarios que son más curiosos por naturaleza, que pueden sentirse felices de conocer cosas nuevas y son ellos las que deberían probar el software libre en primer lugar. Hasta ahora la experiencia indica que una vez que la gente vence sus reservas encuentra que el este software no es muy diferente en su uso al software propietario y está encantada de usarlo. Por ello, es probable que este grupo inicial de usuarios se pase al software libre con entusiasmo. En cualquier caso, esta gente sería también la que proporcione los comentarios y sugerencias más útiles.

El primer grupo de usuarios podría utilizarse en pruebas piloto y una vez que tengan cierta experiencia ya pueden convencer y enseñar a sus colegas. En cualquier caso, ya en la segunda fase, los usuarios que pudieran ser más reservados necesitarán disponer de mayores facilidades de apoyo.

El personal de sistemas en particular, necesita desterrar sus temores desde el comienzo. Serán un punto focal para todos los problemas que indefectiblemente van a aparecer y si no creen en el proyecto no podrán animar a los usuarios de manera positiva.

Pero si el Software Libre es tan robusto y versátil, ¿por qué no acaba de imponerse a los sistemas propietarios, que asfixian con sus licencias a las economías locales y no permiten su mejora por parte de terceros al negar el acceso a sus códigos fuente?

Existen varias explicaciones. En primer lugar está la mera costumbre. Millones de personas en el mundo están habituadas al uso diario de Microsoft Windows que, a menudo, viene pre-instalado

en sus equipos caseros. A muchos niños les educan desde pequeños en las aulas de informática con un ordenador con Windows, de modo que no aprenden exactamente informática sino más bien a desenvolverse dentro de ese sistema operativo.

Otro importante obstáculo para la expansión de los sistemas libres es la enorme difusión de los programas pirateados: si cada empresa y usuario particular tuviera que pagar las licencias de todos los programas propietarios pirateados que utilizan, la expansión del Software Libre aumentaría enormemente. Las tasas de piratería en América Latina oscilan entre un 60-86%.

Tanto el personal de sistemas como los usuarios pueden pensar que no usar el software "estándar industrial" perjudicará su capacidad para desarrollar su carrera. Este es un problema delicado que hay que tratar con mucho cuidado. La administración no querrá verse muy implicada en este enfoque, pero hasta que el software libre sea de uso generalizado, las administraciones se pueden encontrar con el problema descrito con cierta frecuencia.

La gente que conoce los sistemas y configuraciones existentes tiene un cierto poder y podrían sentirse bastante reacios a perderlo si el entorno software libre es muy diferente del existente. Y otra vez aparece la necesidad de una gestión cuidadosa ya que esas personas tienen un papel fundamental en el funcionamiento de los sistemas existentes. Quizá sea necesario que estén entre los primeros en recibir formación sobre los nuevos sistemas para que su posición en la entidad se mantenga.

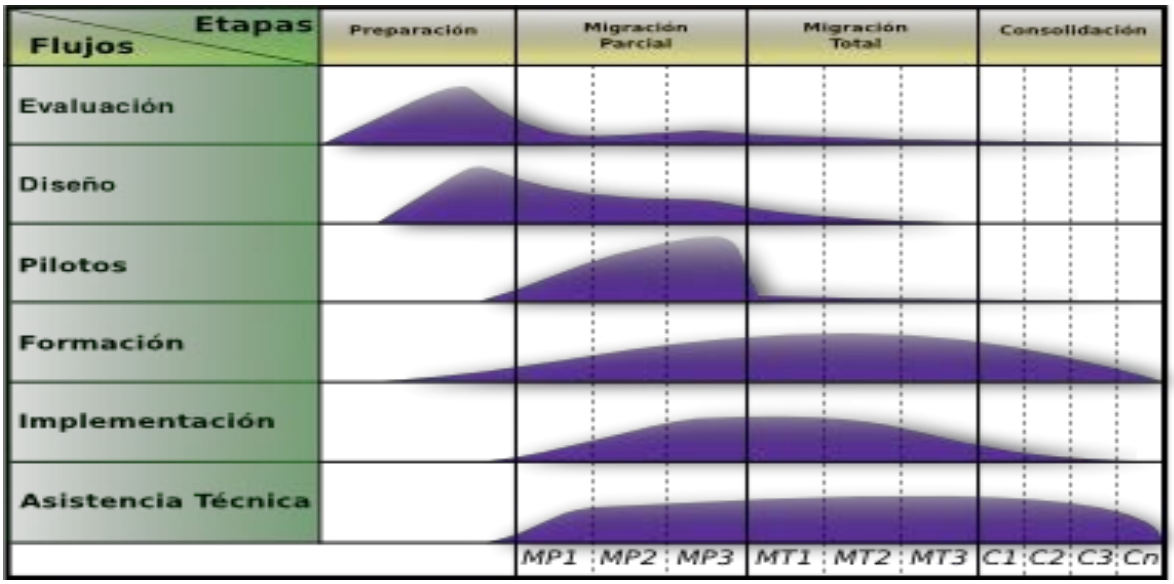
3.3- El proceso ideal.

De manera general, el proceso de migración a Software Libre ideal debe consistir en los siguientes puntos, agrupados en el preciso número de etapas. Algunos de ellos pueden hacerse en paralelo en dependencia de las disponibilidades de las que se disponga a la hora de realizar el proceso.

1. Crear un equipo con la capacitación y el respaldo de gestión adecuados.
2. Entender el entorno final, tanto el software libre como la arquitectura básica, junto con las diferentes opciones y posibilidades disponibles.
3. La migración es una oportunidad de revisar la arquitectura de base así como el software de aplicaciones
4. Entender bien en qué consiste el SWL. Tener claro cuáles son las implicaciones de las licencias para SWL y las diferencias entre las distintas distribuciones.
5. Estudiar los sistemas existentes.
6. Elaborar un caso detallado de migración
7. Consultar a los usuarios. Habilitar un espacio de atención al cliente. Crear un sitio de Intranet con una sección dedicada a "consejos y cómo se hace".
8. Comenzar con proyectos pilotos a pequeña escala, de preferencia en un entorno auto-contenido con pocos usuarios.
9. Decidir sobre la velocidad del proceso de migración una vez iniciado: Todos a la vez; en grupos; o usuario a usuario.
10. Extender la migración a toda la Institución.
11. Supervisar la respuesta de los usuarios y tomar nota de los problemas que surjan.

4. Metodología

La metodología para la migración a Software Libre contempla 4 Etapas y 6 Flujos de Trabajo. Se describe como flujo de trabajo a la secuencia de acciones, actividades o tareas utilizadas para la ejecución de un proceso, incluyendo el seguimiento del estado de cada una de sus etapas y la aportación de las herramientas necesarias para gestionarlo.



ETAPAS.

Preparación: Etapa en la que se realizarán las tareas de recopilación de datos y se lanzará una primera versión de la guía de migración.

Migración parcial: Etapa en la que se realizarán las pruebas y se validará la propuesta a pequeña escala, además de que tendrá gran actividad de trabajo.

Migración total: Cada vez que se ejecute una iteración de esta fase la cantidad de FLOSS irá en aumento, será la etapa que marcará el fin del software privativo.

Consolidación: Etapa que constituirá el soporte al proceso de migración, será el apoyo e indicará los niveles de éxito o fracaso de la Migración a Software Libre.

FLUJOS DE TRABAJO.

Evaluación: Hacer una evaluación de todos los procesos, tecnología y personal y adaptarlas al entorno actual.

Diseño: Diseñar un plan de migración conforme a las necesidades, tomando como partida el resultado anterior.

Pilotos: Poner en marcha el plan en un ambiente real de pruebas.

Formación: Formación del personal y certificación del mismo por niveles de usuarios.

Implementación: Instalación y migración definitiva de servicios y estaciones de trabajo a Software Libre.

Asistencia y soporte técnico: Brindará atención y soporte a las infraestructuras, servicios instalados y al personal.

4.1- Descripción de los flujos de trabajo.

4.1.1- Flujo de trabajo: Evaluación.

La evaluación es donde se realiza una valoración de todos los procesos y tecnologías presentes.

Es de suma importancia pues en él, se definen elementos que serán la base de la futura migración. Este flujo constituye un hito fundamental en el proceso y se realiza una sola vez, teniendo su mayor impacto en esta etapa.

Para este flujo se definen un conjunto importante de tareas:

- Evaluar los tipos de usuarios que participan en el proceso y clasificar los mismos según el grado de impacto, para definir prioridades durante los procesos de formación y concientización, y ver cuales pueden ser partícipes directos o no del proceso.
- Analizar el estado actual de los sistemas informáticos de la institución en cuanto a software y hardware. Para esta tarea puede ser de utilidad, debido a la magnitud de la misma, apoyarse en aplicaciones para automatizar el proceso como pueden ser OCS Inventory. Analizar el estado actual de los servicios que brinda la institución y determinar el grado de criticidad de los mismos para definir prioridades durante el proceso de cambio tecnológico. Evaluar los distintos escenarios posibles que se pueden seguir para acometer la migración.
- Evaluar las potenciales soluciones de migración disponibles para los sistemas informáticos presentes y definir los más adecuados en cada caso, así como definir cuáles precisar desarrollar sus posibilidades reales de funcionamiento.
- Hacer una evaluación de los mecanismos más adecuados que faciliten el soporte y la asistencia técnica dentro de la estructura de la institución.
- Cuantificar las herramientas privativas a migrar. Hacer una evaluación del costo de la migración.

4.1.2- Flujo de trabajo: Diseño.

En este, se definirá el plan de migración de acuerdo a las necesidades requeridas como resultados de la evaluación. Dicho flujo tiene su mayor impacto en la etapa de preparación, aunque es importante destacar que el diseño se redefinirá durante la etapa de migración parcial como retroalimentación de dicha fase.

Constituyen tareas importantes a realizar durante este flujo:

- Establecer un plan concreto de acciones que abarque todos los elementos a migrar.
- Definir una estrategia de sensibilización de acuerdo a los distintos grupos de usuarios, haciendo énfasis en aquellos que mayor impacto poseen en la toma de decisiones, buscando lograr una mejor gestión.
- Diseñar una justificación para el proceso basado en las ventajas y desventajas que posee la utilización de Software Libre.
- Definir los números de usuarios que participan en cada fase del plan.
- Establecer los números y sistemas informáticos que migrarán hacia Software Libre.
- Establecer los períodos de implementación y soporte de las aplicaciones.
- Definir el orden de atención a los usuarios durante la formación según el impacto de los mismos.
- Definir la estrategia para el proceso de instalación soporte y distribución de aplicaciones,

esto incluye gestionar los recursos humanos necesarios, discos de distribuciones a instalar, repositorios, etc.

- Diseñar la ruta de migración. Implementar cada iteración a pequeña escala y validar la configuración propuesta de las aplicaciones.
- Recoger los elementos importantes para introducir mejoras en los distintos puntos de la guía de migración, para ello pueden utilizarse diversos métodos como la encuesta, conversaciones con los usuarios y revisión de los sistemas en funcionamiento.
- Chequear el plan de acciones propuesto.
- Introducir cambios en la guía de migración propuesta.

Lo más importante de este flujo es, además de lo mencionado anteriormente, que permite desarrollar la experticia y la base de conocimiento necesaria para obtener un modelo replicable de migración eficaz y a corto plazo.

4.1.3- Flujo de trabajo: Pilotos.

Una vez que se haya diseñado el plan de migración y con el objetivo de validar su contenido y crear las configuraciones correctas para las aplicaciones, es importante crear un ambiente real de pruebas en un marco reducido, que permita la retroalimentación y los ajustes necesarios de algunas variables del plan propuesto, para poder hacer extensiva la migración con la seguridad de que el número de fallos va a ser mínimo. Es en este punto donde se comprueban en tiempo real el plan de migración y el plan de acción institucional.

Las tareas a acometer durante el flujo son:

- Implementar cada iteración a pequeña escala y validar la configuración propuesta de las aplicaciones.
- Recoger los elementos importantes para introducir mejoras en los distintos puntos de la guía de migración, para ello pueden utilizarse diversos métodos como la encuesta, conversaciones con los usuarios y revisión de los sistemas en funcionamiento.
- Chequear el plan de acciones propuesto.
- Introducir cambios en la guía de migración propuesta.

Lo más importante de este flujo es, además de lo mencionado anteriormente, que permite desarrollar la prueba y la base de conocimiento necesaria para obtener un modelo replicable de migración eficaz y a corto plazo.

4.1.4- Flujo de trabajo: Formación.

Para lograr que los usuarios acepten la transición, lo más importante es que conozcan el nuevo sistema, por lo que la capacitación se convierte en el baluarte fundamental de la migración. El flujo de trabajo de formación estará presente durante toda la migración, comenzando por la justificación del proceso y abarcando hasta las etapas posteriores al soporte, siendo el objetivo fundamental de la misma la capacitación a todo el personal en los nuevos sistemas informáticos que se implantan en la institución.

Como tarea fundamental se propone:

- Confeccionar e impartir planes de formación a los usuarios según el nivel de los mismos, se proponen tres niveles básicos de usuarios que se pueden identificar, esta propuesta puede desglosarse en más niveles en dependencia del lugar:
  - Formación de instructores en Software Libre

- Formación de soporte técnico
- Formación de los usuarios finales
- Formación de desarrolladores

Es importante la creación de un mecanismo de certificación para acreditar cada curso vencido e ir estableciendo determinados niveles en los usuarios para lograr una formación más adecuada.

4.1.5- Flujo de trabajo: Implementación

La implementación es el flujo de trabajo donde se hará efectiva la migración, esta marcará el fin del software privativo según la iteración. De forma paulatina se irán migrando las herramientas e instaurando las aplicaciones y sistemas libres. Es una etapa donde existirán grandes cambios en los sistemas, por lo que la formación y soporte deberá reforzarse. Este será el momento en el que la mayoría de los usuarios podrán tocar de cerca la migración y hacerse partícipes de ella, por lo que todas las medidas que se tomen para el correcto desenvolvimiento de la misma son pocas. Deberán reforzarse las charlas de sensibilización y generar entusiasmo hacia los usuarios con el objetivo de lograr una buena aceptación del proceso.

La implementación de la migración contiene un conjunto de tareas asociadas como otros flujos, algunas de las mismas variarán de un centro a otro en dependencia de las condiciones existentes. Las principales tareas concernientes a esta etapa son:

- Hacer efectiva la migración en dependencia de la iteración, introduciendo los cambios respectivos en la tecnología. Cada equipo migrado y configurado constituye un elemento significativo en el avance de la migración.
- Fortalecer los planes de formación y certificación de usuarios.
- Fortalecer los mecanismos de soporte y mantenimiento.
- Creación de unidades de desarrollo que puedan servir para el desarrollo de aplicaciones locales y la personalización de herramientas e imágenes de GNU/Linux.
- Movimiento masivo de datos hacia los nuevos formatos y sistemas.

4.1.6- Flujo de trabajo: Asistencia y Soporte Técnico.

El último flujo propuesto en la migración es al igual que la formación uno de los más extensos del proceso. La asistencia y soporte técnico estarán presentes a todo lo largo del tiempo que dure el cambio. Su objetivo principal es brindar el apoyo al personal que migra para el mantenimiento de todas la infraestructura. Su carencia o mal funcionamiento podría provocar la recesión de la migración.

La asistencia y soporte técnico debe estar presente el tiempo que sea necesario de acuerdo a las necesidades del lugar, por lo que el número de iteraciones en la fase de consolidación, donde mayor impacto posee dicho flujo, no está definido a ciencia cierta.

Las tareas y acciones más importantes a llevar a cabo en este momento del proceso son:

- Creación de listas, foros y canales IRC de ser posible, para facilitar el debate de temas relacionados.
- Crear canales para la atención a los usuarios vía telefónica ante dudas. Habilitar algún local, stand o espacio físico, a donde puedan dirigirse los usuarios a recibir asesoría.
- Creación y mantenimiento de sitios y cursos virtuales para el auto-aprendizaje y la auto-certificación.
- Creación de repositorios de aplicaciones, datos, y servicios asociados: personalización de

repositorios, secciones propias, etc.

- Creación de manuales, FAQs, Como hacer.
- Creación, de acuerdo a las posibilidades del centro, de comunidades virtuales en la red.
- Establecer para los centros en los que se realicen desarrollo, políticas que promuevan el uso de estándares para la creación de aplicaciones, como pueden ser librerías gráficas, ejemplo: wxwidgets o foxtoolkit y lenguajes de programación como: ANSI C, Java, PHP y otros.
- Realización de estudios de las aplicaciones más usadas y de las necesidades de los usuarios, a fin de lograr mejoras en el servicio de aplicaciones, optimización de las mismas para aumentar su rendimiento y saber en cada momento cuales son las necesidades de los clientes.
- Creación de un portal informativo como centro del proceso que integre los métodos mencionados anteriormente y contenga un Service–Desk o escritorio de servicios, para aumentar los tiempos de respuesta ante las preguntas más frecuentes.

Lograr la automatización de la mayor cantidad de tareas, por ejemplo implantar mecanismos para la actualización automática de los repositorios, instalar herramientas que permitan la instalación automática de herramientas en las maquinas de los clientes, etc.

4.2- Alternativas de migración.

En la determinación de las alternativas de migración de los sistemas de información a software libre, será necesario analizar una serie de elementos, entre los que se encuentran:

- La disponibilidad presupuestal con la que cuenta la institución para la ejecución del proyecto de migración.
- La factibilidad total o parcial de migración de los sistemas de información existentes en la institución.
- El hardware que contiene a los sistemas de información.
- La cantidad y calidad de los recursos humanos disponibles.

La bibliografía consultada coincide en la existencia de dos rutas para la realización de la migración.

RUTA 1- Añadir estaciones GNU/LINUX a los dominios Windows existentes e ir trasladando gradualmente los datos y los usuarios, y luego eliminar los antiguos servidores propietarios. Es posible transferir a clientes y servidores independientemente. Añadir servidores al dominio Windows es uno de los modos más rápidos de sacar provecho del sistema libre.

RUTA 2-Construir una infraestructura paralela de tipo GNU/LINUX y transferir a los usuarios y sus datos en grupos, con mínima interacción entre el sistema antiguo y el nuevo. Es mucho más sencillo que ejecutar un sistema mixto GNU/LINUX-Windows, pero crea una cooperación entre la gente que usa Windows y la que usa sistemas GNU/LINUX más difícil.

4.2- Levantamiento de Información.

Para la realización del Levantamiento de Información se pueden emplear todo tipo de variante incluido el uso de planillas impresas que recojan los principales datos de interés. Lo importante es que se disponga de toda la información posible y pueda ser procesada por el equipo técnico en la toma de decisiones.

Esta guía propone el uso de un software de inventario: OCS INVENTORY. Es una aplicación web que se instala en su modalidad cliente en cada uno de los ordenadores y cuya ejecución envía todo tipo de datos de hardware y software a su variante servidor. Es completamente libre, puede descargarse de internet y ser sometida a transformaciones, a fin de generar los reportes de información necesarios.

4.3- Plan de migración.

Es el documento rector de todo el proceso de migración recogiendo en su contenido:

- La información general del organismo: Misión, Visión y Objetivos de la entidad y cada uno de los organismos que puedan conformarla.
- Los proyectos de acción a corto, mediano y largo plazo: Objetivo general y Objetivos específicos con sus acciones y metas correspondientes.
- Informe de la situación de la entidad (a partir del Inventario) para la realización de la migración.
- La forma en la que se migrarán los servicios a partir de las particularidades de la entidad.
- La forma en la que se migrarán las bases de datos a partir de las particularidades de la entidad.
- La forma en la que se migrarán las estaciones de trabajo a partir de las particularidades de la entidad.
- Aplicaciones informáticas que sustituirán a las utilizadas en software privativo, así como la forma en que se emularán las que no tengan equivalente libre y los pasos a acometer para la migración de los sistemas de gestión adquiridos a empresas productoras o producidos por personal del propio centro.
- Planificación de tiempo, recursos materiales, personas involucradas.

- Plan de capacitación del personal: estrategias de capacitación, materias de capacitación.
- Forma en que se dará soporte.
- Estimaciones Generales: costos, tiempo, numero de personas, recursos.

4.4- Laboratorio de formación, capacitación y soporte.

Las labores relacionadas con la formación y capacitación del personal, tienen sus primeras acciones en esta etapa, una vez que se ha procesado el potencial de recursos humanos con que se cuenta.

En la medida de lo posible, cada institución debería ser capaz de montar un laboratorio con un determinado números de computadoras con el objetivo de convertirlo en cuartel general de todo el proceso, zona de las pruebas pilotos, centro de la capacitación y lugar de soporte.

4.5-Migración parcial

El primer momento es la implantación de Software Libre en los servidores de la institución.

Luego de tener la infraestructura de servidores completamente en FLOSS (Free Libre Open Source Software, siglas en ingles), se propone el uso de herramientas libres en el sistema actual (Microsoft Windows), esto permitirá que los usuarios puedan probar las herramientas con las que trabajarán en GNU/Linux en un entorno ya conocido, teniendo la posibilidad de capacitarse en el uso de estas herramientas sobre este entorno y de ir facilitando la conversión de archivos a formatos estándares, para evitar problemas de compatibilidad entre las aplicaciones. Entre las aplicaciones libres que pueden sustituir a las aplicaciones que comúnmente se utilizan en Windows están:

Finalidad	Software Privativo	Software Libre
Editor de diagramas	MS Visio	Dia
Ofimática	MS Office	OpenOffice.org
Gestión de finanzas	MS Money	GNUCash, Grisbi
Gestión de proyectos	MS Project	DotProject
Maquetación	FreeHand, Adobe Ilustrator	Scribus
Agenda y calendario	MS Outlook	Mozilla Sunbird
Cliente de correo	MS Outlook	Mozilla Thunderbird
Navegadores	Internet Explorer	Mozilla Firefox
IRC	Xchat	XChat
Mensajería instantánea	Pandion, MSN	Pidgin, aMSN
Bases de datos	MS SQL	PostgreSQL, MySQL
Desarrollo .NET	Visual Studio .NET	Mono
Desarrollo C/C++	C++ Builder	Code::Blocks
Desarrollo python	WingIDE	SPE
Editores	Notepad	Scite
UML	Rational Rose	ArgoUML
Gráficos 3D	3DMax	Blender
Gráficos 2D	Adobe Photoshop	Gimp
Herramienta CAD	AutoCAD	FreeCAD
Fuentes	Arial	Bitstream Vera, DejaVu
Video y multimedia	Windows Media Player	Mplayer, VLC, Totem
Gráficos infantiles	Paint	TuxPaint
Antivirus	Nod 32, Kasperky	ClamWin

Una vez que los usuarios estén ya entrenados en el uso de las herramientas libres con las que interactuarán sobre GNU/Linux y convencidos de las ventajas de utilizar FLOSS se propone el

cambio de la base y la instalación de GNU/Linux como nuevo sistema operativo a usar, lo que demanda gran atención por parte de todos los implicados en la tarea, pues es aquí donde más "frágil" resulta la migración.

Complementariamente, se puede utilizar la virtualización para algunas herramientas, con el objetivo de hacer pruebas. Es importante tener en cuenta que la migración tal vez no se realice de forma total, debido a la existencia de aplicaciones que no poseen equivalente libre, en tal caso se pueden utilizar aplicaciones como Wine, que permiten emular software de Windows sobre GNU/Linux; unificar varias herramientas libres para lograr los mismos resultados que la propietaria o la re-programación de la misma.

4.6- *Nova: Distribución cubana de Software Libre.*

La idea de crear una distribución de GNU/Linux surge de un grupo de estudiantes de la Universidad de las Ciencias Informáticas, como respuesta a la necesidad de una plataforma que garantizara la compatibilidad del software que se estaba desarrollando, con los sistemas libres que tanto auge tienen en el mundo actual. Posteriormente el proyecto se volvió más ambicioso con la inminente migración a software libre de algunos organismos estatales y ministerios, convirtiéndose en una plataforma para generar distribuciones a la medida.

En estos momentos Nova tiene como objetivo la creación de un sistema operativo, no la mera personalización de una distribución. Se aspira a proveer un producto orientado a usuarios inexpertos que hayan tenido que migrar de Microsoft Windows a entornos GNU/Linux o cuya experiencia con computadoras sea nula. Se pretende automatizar la mayor cantidad de procesos posible, de forma que la interacción del usuario con el sistema sea fácil e intuitiva y facilite el proceso de transferencia de conocimientos y aprendizaje, algo tan difícil cuando se trata de asimilar nuevas tecnologías.

Debido a los apenas 3 años del proyecto Nova, su utilización es relativamente reciente en algunas instituciones interesadas en migrar de forma paulatina a software libre.

La probabilidad de infección del sistema NOVA por parte de programas maliciosos es casi nula, incluso sin tener instalado un antivirus, por tanto no se daña el sistema por esta causa tan frecuentemente como ocurre al hacerse uso del software privativo. En cuanto al consumo y falta de espacio para la instalación o compilación de programas, no sería una preocupante a tener en cuenta debido a que la mayor parte de los programas o software necesarios ya están pre-compilados, y se llevan una menor capacidad de almacenamiento a la hora de ser instalados. A todo lo anteriormente mencionado, se le debe sumar que las aplicaciones no requieren supervisión tan estrecha ni pagos de pólizas de mantenimiento, necesarias para obtener las actualizaciones de los productos (Service Packs); los cuales pueden contener actualizaciones

para la estabilidad del sistema, la compatibilidad del programa, la seguridad, etc.

El sistema operativo NOVA por ser un sistema libre presenta las características de los mismos, siendo por ello muy robusto, estable y rápido. Ideal para servidores y aplicaciones distribuidas. A esto se añade que puede funcionar en máquinas humildes: alcanza ejecutar servicios en un x86 a 200 MHz con calidad. Presentando además la posibilidad de modificación y la variedad de programas que se pueden seleccionar en Internet o en el repositorio de la distribución, de acuerdo a las necesidades del cliente.

Al ser una plataforma estable y segura, es favorecido también el desempeño de aplicaciones de todo tipo tales como: bases de datos, aplicaciones XML, multimedia, la rápida navegación por la Web, y la velocidad de las aplicaciones, muy superiores a los sistemas Windows.

4.7-Migración total

La migración total debe llevarse a cabo siguiendo los mismos pasos que durante la migración parcial, salvo que en esta se despliegan las soluciones de migración a la totalidad de los locales y dependencias de la entidad siguiendo el organigrama de la misma. Es una etapa compleja por la concentración de flujos de trabajo que concurren en la misma. Su avance implica, la inclusión de un mayor número de personas, el cumplimiento exacto del cronograma de trabajo y la elaboración de la documentación de todo el proceso.

Deben seguirse con detenimiento las “disposiciones” contempladas en el Plan de Migración y estarse atento a cualquier irregularidad que pueda presentarse y que no fue detectada a pesar de haberse realizado todo un período de pruebas previamente y que tal vez requiera que se recurra a métodos o soluciones con las que no se contaba. Resulta vital prestar atención a las opiniones de los usuarios y recopilar cualquier tipo de quejas o inconvenientes, a fin de solucionarlos cuanto antes, evitando retrasos innecesarios y la recesión del proceso.

4.8-Consolidación

A lo largo del proceso de migración ha quedado evidenciada la necesidad de acometer en todo momento la formación y capacitación de usuarios, comenzando incluso desde etapas tempranas y manteniéndola aún después de concluida la misma, a fin de generar recursos para el aprendizaje y documentar todo lo realizado. Cuestiones que aunque no lo parezcan, tienen un alto valor agregado y constituyen ahorros considerables para la institución y fuente de generación de ganancias, en caso de ser usadas con esos fines.

Cada institución, en dependencia de sus características, elaborará y pondrá en práctica su propia estrategia de capacitación, dando especial prioridad a las cuestiones relacionadas con su hacer diario, así como, a las tecnologías que en un futuro inmediato se introducirán en el ambiente laboral.

Pensando más en grande, los usuarios avanzados podrían acceder a programas internacionales de certificación de usuarios, supervisados por el Linux Professional Institute. Esto permitirá a la institución ganar prestigio y posicionarse en un buen lugar en el mercado.

El programa de formación LPI de Linux Professional Institute está especialmente diseñado para proporcionar los conocimientos y habilidades necesarios para administrar cualquiera de las distribuciones de los sistemas operativos Linux y sus herramientas asociadas.

Anexo 1-Selección de referencias sobre la importancia y el papel de la información, realizadas por el líder de la Revolución Fidel Castro Ruz.

1. "Debemos estar al tanto de lo que se publica en el mundo sobre todo tipo de materia que sea de interés para el país, de manera que haya una información..."[126]
2. "Conocemos demasiado bien los latinoamericanos esos hechos…los conocen sobre todo quienes tienen que sufrir esas mentiras, esa información al servicio de las peores causas imperialistas, que son las únicas que pueden leer pueblos enteros en este continente. Y eso forma parte del mecanismo imperialista, porque esas agencias cablegráficas mentirosas, truculentas, fraudulentas, forman parte —¡forman parte!— de la maquinaria del imperialismo, forman parte de los instrumentos que emplea el imperialismo para llevar a cabo su política"[127]
3. "Vean ustedes cómo incluso nuestra industria azucarera, tradicional e histórica, necesita de la técnica moderna, necesita de la electrónica, necesita de las computadoras, para poder realizar el trabajo en condiciones óptimas**"**.[128]
4. "Nos interesa sobre todo que las masas tengan información y que las masas comprendan y que las masas se dispongan a librar su batalla… solo el pueblo y solo con el pueblo, con la toma de conciencia del pueblo, la información del pueblo, la decisión del pueblo y la voluntad del pueblo, esos problemas podrán ser superados"[129]
5. "Ojalá llegue el día en que otras circunstancias nos permitan un manejo de todos los datos de carácter económico, para que las masas tengan todos los datos al día: cuánto gastamos en tal producto, en tal otro, cuánto se importa, cuánto se exporta, cuánto gastamos por aquí, cuánto gastamos por allá. Es decir que podamos manejar la información esa ampliamente; porque con la información y la información en manos de las masas, se pueden tomar todas las medidas"[130]
6. "Las oficinas de información de Estados Unidos …se gastan cientos de millones de pesos en difundir literatura, imprimir libros, hacer programas de prensa, de radio, de televisión, de cine, y esos programas los exportan. ¿Y qué traen? Ideología reaccionaria. ¿Qué traen? Cultura antinacional. ¿Qué traen? Todo aquello que pueda envenenar el alma del pueblo, todo aquello que pueda reblandecer al pueblo, todo aquello que pueda confundir al pueblo, todo lo que pueda engañar al pueblo, todo lo que signifique desarmar espiritualmente al pueblo"[131]
7. "Y un pueblo —tengan la seguridad— no solo será más rico mientras más fábricas posea, o más minerales, o más materias primas descubra: un pueblo será por encima de todo más

[126] Discurso pronunciado en el acto clausura del XI Congreso médico y VII estomatológico nacional, el 26 de febrero de 1966.

[127] Discurso pronunciado en la clausura de la primera conferencia de la Organización Latinoamericana de Solidaridad, el 10 de agosto de 1967.

[128] Palabras a los soldados y oficiales de las Fuerzas Armadas Revolucionarias que tomarán parte en la Zafra de los 10 Millones. 4 de noviembre de 1969

[129] Discurso pronunciado en la conmemoración del XVIIaniversario del asalto al cuartel Moncada, el 26 de julio de 1970

[130] Discurso pronunciado en el acto central por el Día Internacional de los Trabajadores, el 1ro de mayo de 1971

[131] Discurso pronunciado en la plaza mayor de la ciudad de Valparaíso, Chile, el 30 de noviembre de 1971

rico cuanto más cultura política tenga, cuanto más preparación tenga, cuanto más información tenga…"[132]

8. "Un sistema con computadoras, computadoras que pensamos que tengan un buen banco de información y que, además, puedan conectarse con las computadoras de países socialistas, para recibir vía satélite informaciones que nos interesen del exterior"[133]
9. "Han estado adoptando medidas para atentados personales, de una manera bastante descarada, pero lo sabemos, y una buena información es muy importante en todo"[134]
10. **"**…miremos a largo plazo, y prestemos la mayor atención a la enseñanza y a la utilización de las técnicas de computación… El desarrollo industrial y social requiere que nos posesionemos ambiciosamente de esas técnicas…"[135]
11. **"**El socialismo va a ser muy difícil de construir plenamente sin la computación…"[136]
12. "…a todos nos duele la forma en que a través del control de los medios masivos de difusión, de las transnacionales de la información, nos informan lo que ellos quieren que nosotros conozcamos, y matizado de la forma que les interesa que nosotros lo conozcamos. Todos los días no solo nos roban, todos los días nos envenenan a través de sus agencias transnacionales, todos los días agreden nuestra cultura"[137]
13. "Discutiendo con los periodistas, les digo: ¿Y por qué no pensamos en la esencia, en el fondo de los problemas? Porque no solo nos explotan, nos desinforman de una manera terrible. Me quedo asombrado de la ignorancia que hay sobre muchos problemas; por las preguntas que nos hacen sobre Cuba, nos damos cuenta de que hay una ignorancia tremenda, lo veo en las preguntas de los periodistas…A nosotros muchos amigos nos dicen: Ustedes deben informar más de lo que ocurre en Cuba. Digo: Sí, nosotros queremos, ¿pero con qué?, si son poderosísimas agencias de información, medios masivos, cantidad de decenas de miles de millones los que manejan todos los años; son los informadores del mundo, mientras el mundo no sabe lo que está pasando en nuestros países. Y a uno le duele, realmente, cuando ve de qué manera desinforman y engañan, en esta era moderna de las comunicaciones, porque sencillamente los grandes medios de información del mundo están en manos de ellos, ¡están en manos de ellos!, y se hace difícil, incluso, conocer la verdad. Son realidades"[138]
14. "…no desperdiciamos ocasión ni oportunidad de adquirir conocimientos desde el exterior, de buscar información y de utilizar todo lo que sea útil en el mundo, ya que por mucho que sepamos de algo o nos creamos que sabemos de algo, siempre tenemos que ir al resto del mundo a buscar aquellas cosas que la inteligencia humana ha creado y que puedan ser también útiles para nosotros"[139]

---

[132] Discurso pronunciado en el acto celebrado con motivo de la terminación del montaje de una unidad en Tallapiedra de la Empresa Eléctrica, el 23 de julio de 1972

[133] Clausura del claustro nacional de Ciencias Médicas. 16 de abril de 1983

[134] Dialogo sostenido con delegados a la conferencia sindical de los trabajadores de América Latina y el Caribe sobre la deuda externa, el 18 de julio de 1985

[135] Discurso por el XXXI Aniversario del Asalto al Cuartel Moncada. 26 de julio de 1985

[136] Discurso en la clausura del V Congreso de la Unión de Jóvenes Comunistas. 5 de abril de 1987

[137] Discurso pronunciado en la clausura del III encuentro continental de mujeres, el 7 de octubre de 1988

[138] Discurso pronunciado en el acto de entrega del premio Estado de Sao Paulo al etnólogo Orlando Villas Boas, en Brasil, el 17 de marzo de 1990

[139] Discurso pronunciado en la clausura de la asamblea de balance del trabajo, renovación y ratificación de mandatos del PCC en Ciudad de La Habana, el 7 de noviembre de 1993

15. “Hay datos, incluso, que no se pueden andar divulgando, hay que mantenerlos con cierta discreción, porque no se le puede estar dando información al enemigo gratuitamente. ¡Que la averigüe si puede!”[140]
16. “En materia de información, ustedes lo mencionaron en una de las comisiones, el fenómeno de la producción audiovisual para la recreación es hoy día un monopolio casi exclusivo de Estados Unidos, que ha desplazado a Europa y a todo el mundo prácticamente de ese mercado, cuyos productos conocemos, algunos buenos, y una enorme masa de veneno de toda clase…Ahora se habla ya de las autopistas de la información, cuestiones nuevas que servirán para calzar, a través de la propaganda y a través de la influencia sobre la mentalidad humana, este orden económico que quieren imponerle al mundo.”[141]
17. “No se podrá sobrevivir sin ese dominio de la computación, de la electrónica, de los medios de comunicación.”[142]
18. “Hay que seguir sin tregua en la búsqueda de información sobre las características de cada arma nueva que hagan, porque van a seguir haciendo armas nuevas…”[143]
19. “Hay que insistir siempre en la necesidad no de inventarlo todo, pero sí debemos estar informados de todo. Ahora existe Internet, cualquier información se puede obtener en cuestión de minutos de cualquier parte del mundo; un científico nuestro en un centro de investigación puede buscarla lo mismo en China, que en Japón, que en cualquier otro lugar, y eso sí que no se puede bloquear. No nos pueden bloquear la obtención de conocimientos”[144]
20. “Planteada la lucha de ideas a nivel mundial, muchas veces no se tiene acceso a los medios de divulgación masiva controlados por las grandes transnacionales, o no se tiene acceso a las grandes cadenas de televisión o de información; pero siempre hay alguna forma de hacer llegar el mensaje al mundo, siempre hay alguna posibilidad, y mientras más se desarrollen las comunicaciones, ello es más posible… una computadora conectada a la red de Internet es ya una posibilidad de hacer llegar un mensaje, un pensamiento a millones de personas en el mundo”[145]
21. “Estados Unidos no solo tiene espías en cantidades industriales y gente de la CIA dedicada todo el tiempo a eso y a la subversión en su Oficina de Intereses en Cuba … sino que sostiene relaciones con elementos y grupúsculos contrarrevolucionarios, con los cuales colabora y de los cuales recibe información. Tiene todo un sistema de espionaje montado… un espionaje técnico colosal por medio de satélites, por medios radioelectrónicos y de todo tipo, captando comunicaciones y buscando información. Capta todas las llamadas cubanas; no hay conversación que yo pueda sostener con cualquier dirigente latinoamericano o cualquier político en el exterior que no sea captada por Estados Unidos. Estamos sometidos a un espionaje total y feroz… A nosotros nos llegan informaciones por distintas vías; nosotros recibimos informaciones porque hay

[140] Discurso pronunciado en la clausura del VI Congreso de la Federación de Mujeres Cubanas, el 3 de marzo de 1995
[141] Discurso pronunciado en la clausura del festival juvenil internacional cuba vive, el 6 de agosto de 1995
[142] Discurso pronunciado en la clausura del II Congreso de de los pioneros. 20 de julio de 1996
[143] Discurso pronunciado en la clausura del XI Foro de ciencia y técnica, el 21 de diciembre de 1996
[144] Discurso pronunciado en la clausura del V Congreso del Partido Comunista de Cuba. 10 de octubre de 1997
[145] Discurso pronunciado en la clausura del evento internacional Economía'98, el 3 de julio de 1998

muchos amigos de Cuba en Estados Unidos: hay norteamericanos que son amigos de Cuba, hay gente de países latinoamericanos que viven en Estados Unidos y son amigas de la Revolución, se oponen al terrorismo, se oponen a todas esas cosas. Hay personas que espontáneamente, de manera absolutamente espontánea —porque jamás Cuba ha obtenido información mediante empleo de dinero, ni ha tenido informantes pagados ni nada parecido—, han colaborado con nuestro país y han brindado informaciones a Cuba. …¿Pero qué nos interesa a nosotros de Estados Unidos? ¿Qué información nos interesa de Estados Unidos? Exclusivamente información sobre las actividades terroristas contra Cuba; información sobre los planes de sabotajes, de los que han realizado muchos; introducción de explosivos, de armas procedentes de Estados Unidos, de lo cual tenemos montones de pruebas; introducción de virus y bacterias desde Estados Unidos, es decir, guerra bacteriológica y, muy especialmente, graves actos terroristas organizados contra el país desde Estados Unidos. Sí, a veces hemos enviado ciudadanos cubanos que se han filtrado en organizaciones contrarrevolucionarias, para informar de actividades destructivas contra nuestra patria, y creo que tenemos derecho a hacerlo mientras Estados Unidos tolere que desde allí se organicen sabotajes, incursiones armadas, ametrallamiento de instalaciones turísticas, introducción de armas, explosivos y, sobre todo, brutales atentados terroristas. Sí, a veces han marchado cubanos pero a buscar exclusivamente la información que nos interesa. Creo que la mala fe en esto consiste en haber pretendido presentar el problema como una búsqueda de información sobre las fuerzas armadas y sobre las actividades del ejército de Estados Unidos."[146]

22. "Hay que aprender, y se aprende oyendo, no hablando. Hablando se puede ejercitar un poco la mente, pero escuchando se recoge información, ideas, puntos de vista y se aprende. Lo que uno escucha es la materia prima de lo que se puede elaborar después en el cerebro… Nos interesa mucho recoger la información, las opiniones."[147]
23. **"…**el 60% de las redes mundiales y el 75% de Internet. Todo eso está en manos de ellos, y todo eso está al servicio de las concepciones de la globalización neoliberal y de las ideas estas que están planteando. Son fuentes de ideología poderosísimas, de información, creencias, costumbres, capaces de transformar muchas cosas**"**[148]
24. "Vivimos una etapa en que los acontecimientos marchan por delante de la conciencia de las realidades que estamos padeciendo. Hay que sembrar ideas, desenmascarar engaños, sofismas e hipocresías, usando métodos y medios que contrarresten la desinformación y las mentiras institucionalizadas"[149]
25. "En consecuencia es necesario trabajar Internet, apoderarnos de Internet, un sistema que inventaron los ricos y que debemos aprovechar y lo estamos aprovechando"[150]
26. "…en este mundo que llaman globalizado, donde, entre otras cosas, las más globalizadas son la desinformación y la mentira… Quien tenga el hábito de informarse, de emplear dos o tres horas todos los días en recoger y analizar información de lo que ocurre en el

[146] Entrevista concedida a Lucía Newman, de la CNN, en el hotel Porto Palacio, Portugal, el 19 de octubre de 1998

[147] Entrevista concedida a la prensa nacional e internacional, el 23 de junio de 1998

[148] Conferencia Magistral en el acto convocado por la Universidad Autónoma de Santo Domingo. 24 de agosto de 1998

[149] Discurso en el acto central por el cuadragésimo aniversario del triunfo de la Revolución, el 1ro de enero de 1999

[150] Palabras en el VII Congreso de la Unión de Periodistas de Cuba. 14 de marzo de 1999

mundo, tiene idea de cómo funcionan los mecanismos de sembrar mentiras y de crear desinformación… En realidad, al campo socialista y a la URSS no los destruyeron fundamentalmente sus propios errores, los destruyó esa infernal maquinaria de la mentira, del engaño y de la desinformación… hoy ya todo el mundo admite que la inteligencia, los conocimientos, la información son el factor fundamental del desarrollo… Hay medios de contrarrestar el gigantesco poder del monopolio de los medios de información y de los dueños; los esclavos, los periodistas, los proletarios de la prensa tienen por delante posibilidades infinitas."[151]

27. "Es urgente enfrentar la situación de indigencia en que nuestro grupo de países se encuentra en este escenario de las redes globales de información, Internet y todos los medios modernos de transmisión de información e imágenes… Conectarnos al conocimiento y participar en una verdadera globalización de la información que signifique compartir y no excluir, que acabe con la extendida práctica del robo de cerebros, es un imperativo estratégico para la supervivencia de nuestras identidades culturales de cara al próximo siglo"[152]
28. "Cada vez que podemos transmitir un mensaje, lo transmitimos por todos los medios. Aunque ellos son los dueños de los medios masivos más importantes del mundo, de los medios de comunicación, nosotros, los pobrecitos, tenemos posibilidades de hacer llegar nuestros mensajes de distintas formas. Nosotros en nuestra batalla contra el bloqueo y contra otras muchas cosas, podemos hacer llegar a través de satélites a muchos centros universitarios de este país nuestro mensaje. Y por Internet, a cualquier rincón de la tierra."[153]
29. "Los médicos de nuestro país tendrán oportunidad de acceso, al menos, a 18 revistas mensuales, entre cubanas y extranjeras, y a cualquier información, cualquier libro, cualquier obra sobre la salud, es algo, e incluso un médico de Baracoa, si quiere, puede consultar a un eminente especialista que vive en la capital y pueden producirse conferencias a través de esa red. El personal docente en su momento tendrá también una red similar para hacer las consultas necesarias. Las universidades podrán hacer milagros**"**[154]
30. "Internet, a través de su famosísima fibra óptica, está comunicando todos los continentes, de lo cual nos alegramos, para poder trasmitir nuestras verdades y nuestros mensajes"[155]
31. "Si se habla de un diluvio universal sería incorrecto, pues en todo caso podría hablarse de dos diluvios: el de la Biblia, y este diluvio universal de información, que muchas veces se transforma en un diluvio universal de mentiras, un diluvio universal de engaños; y digo muchas veces, no siempre, es justo hacer constar excepciones"[156]

[151] Discurso en la clausura del VII congreso de la Federación Latinoamericana de Periodistas el 12 de noviembre de 1999

[152] Mensaje a los participantes en la reunión ministerial del Grupo de los 77. 19 de septiembre de 1999

[153] Palabras en la Mesa Redonda No. 3 de la Cumbre del Milenio de la ONU, "El papel de las Naciones Unidas en el Siglo XXI". 7 de septiembre de 2000

[154] Discurso en la clausura del Tercer Congreso Pioneril. 9 de julio de 2001

[155] Palabras en el acto de puesta en marcha del sistema de interconexión eléctrica que suministrará energía a la zona del norte de Brasil. Santa Elena de Uairen, República Bolivariana de Venezuela. 13 de agosto de 2001

[156] Discurso en la clausura del IV Encuentro Internacional de Economistas. 15 de febrero de 2002

32. "Que la humanidad no tiene otra alternativa que cambiar de rumbo, es algo que no puede dudarse…En esto el factor subjetivo deberá desempeñar su papel más importante, y para ello debe ser informado e incitado a pensar. Transmitir información, alentar debates, crear conciencia, será tarea de los más avanzados"[157]
33. "El último plan de atentado fue en la reunión aquella de Panamá, organizado y dirigido por Posada Carriles, el autor de la voladura del avión de Barbados…Lo descubrimos por métodos de penetración, búsqueda de información y hasta por métodos técnicos. Nosotros también podemos saber de dónde está hablando alguien con un celular…"[158]
34. "Ha aparecido Internet y el valor de las grandes cadenas ha ido disminuyendo. Los grandes órganos que antes estaban monopolizados han ido disminuyendo su influencia monopólica, porque al surgir y masificarse Internet, que está en manos de muchas personas de las capas medias, en realidad las posibilidades de trasmitir otros mensajes son hoy enormes…Se nos pueden hacer todas las críticas que se quieran y opinar sobre cualquier cosa; pero el problema es que lo que se conoce de Cuba es una información que ha sido deformada durante mucho tiempo, aplicando toda una técnica para deformar la verdad y vender mentiras"[159]
35. "Estamos creando un sistema de Intranet en Cuba, con unas 5 000 computadoras, que pondrá al acceso de todos los médicos cualquier información, la última información del mundo en una revista, en un libro, la posibilidad de consulta, la posibilidad de conferencias"[160]
36. "…debemos tener valor de decir las verdades, y no todas, porque usted no está obligado a decirlas todas de una vez, las batallas políticas tienen su táctica, la información adecuada, siguen también su camino. Yo no les voy diciendo todo, yo les voy diciendo lo que es indispensable"[161]
37. **Vanessa Davies**- ¿Cuáles son las armas ahora para hacer la revolución …?
    Fidel Castro.- Divulgar la realidad de lo que va a ocurrir y te voy a decir por qué.
    Vanessa Davies .- ¿La comunicación es el arma?
    Fidel Castro.- Bueno, yo creo que ustedes tienen el arma nuclear en las manos, ideológica, y si ganan esa batalla habrán derrocado al régimen, y no harán falta las revoluciones[162]
38. La ausencia de la verdad y la prevalencia de la mentira es la mayor tragedia en nuestra peligrosa era nuclear"[163]

[157] Discurso en la clausura del V Encuentro sobre Globalización y Problemas del Desarrollo. 14 de febrero del 2003
[158] Comparecencia especial en la Mesa Redonda el 25 de abril de 2003
[159] Entrevista concedida al diario Clarín. Buenos Aires, Argentina, el 26 de mayo del 2003
[160] Discurso en la clausura del VI Congreso de los CDR. 28 de septiembre de 2003
[161] Discurso en el acto por el aniversario 60 de su ingreso a la universidad, efectuado en el Aula Magna de la Universidad de La Habana, el 17 de noviembre de 2005
[162] Entrevista concedida a periodistas venezolanos. 8 de agosto 2010
[163] Reflexiones del compañero Fidel "La infinita hipocresía de Occidente" 12 de septiembre de 2010

Anexo 2- Decreto Ley No. 199/1999 “Sobre la seguridad y protección de la información oficial”

CONSEJO DE ESTADO

FIDEL CASTRO RUZ, Presidente del Consejo de Estado de la República de Cuba.

HAGO SABER: Que el Consejo de Estado ha acordado lo siguiente:

POR CUANTO: Los servicios especiales extranjeros dedican cuantiosos recursos, medios sofisticados y fuerzas cada vez más preparadas en la obtención de informaciones de interés, lo que hace necesario fortalecer las medidas establecidas para la seguridad y protección de la información oficial, que pudiera ser útil para los planes subversivos y agresivos contra la República de Cuba.

POR CUANTO: Los cambios que se han producido a partir de la reorganización de los Organismos de la Administración Central del Estado y la creación de las nuevas formas de relaciones económicas, aconsejan la introducción y puntualización de medidas encaminadas a lograr una mejor eficiencia en la protección de la información oficial.

POR CUANTO: El desarrollo de las comunicaciones y tecnologías de información en el país exige, para transmitir y almacenar información oficial clasificada, la aplicación de medidas de Protección Criptográfica y de seguridad Informática, cuyo diseño y aplicación requieren de una alta especialización y centralización estatal.

POR CUANTO: La Ley número 1246 del Secreto Estatal del 14 de mayo de 1973 sobre la Protección del Secreto Estatal y su Reglamento, puesto en vigor por el Decreto número 3753 del 17 de enero de 1974; el Decreto número 3787 del 23 de septiembre de 1974 que puso en vigor los Reglamentos Gubernamentales para el Servicio Cifrado Nacional y para el Servicio Cifrado Exterior, así como otras disposiciones complementarias en esta materia requieren ser adecuadas a las nuevas condiciones y cambios que tienen lugar en el país, en función de lograr una mayor seguridad y protección de la información.

POR CUANTO: El Consejo de Estado, en uso de la atribución que le confiere el Artículo 90, inciso c) de la Constitución de la República, resuelve dictar el siguiente:

DECRETO LEY No. 199/1999

SOBRE LA SEGURIDAD Y PROTECCIÓN DE LA INFORMACIÓN OFICIAL

CAPITULO I

Objetivos y Definiciones

ARTICULO 1.- El presente Decreto-Ley tiene como objetivo, establecer y regular el Sistema para la Seguridad y Protección de la Información Oficial, cuyas normas deben cumplimentar tanto órganos, organismos, entidades o cualquier otra persona natural o jurídica residente en el territorio nacional, como las representaciones cubanas en el exterior.

ARTICULO 2.- El sistema para la seguridad y Protección de la Información Oficial comprende la clasificación y desclasificación de las informaciones, las medidas de seguridad con los documentos clasificados, la Seguridad Informática, la Protección Electromagnética, la Protección

Criptográfica, el Servicio Cifrado y el conjunto de regulaciones, medidas, medios y fuerzas que eviten el conocimiento o divulgación no autorizados de esta información.

ARTICULO 3.- En el presente Decreto-Ley se emplean, con la acepción que en cada caso se expresa, los términos y definiciones siguientes:

a) **Acceso**: Facultad o autorización que se otorga a una persona y que le permite conocer información oficial clasificada para el ejercicio de sus funciones.

b) **Auditoria a la Seguridad Informática**: Es el proceso de verificación y control mediante la investigación, análisis, comprobación y dictamen del conjunto de medidas dirigidas a prevenir, detectar y responder a acciones que pongan en riesgo la confidencialidad, integridad y disponibilidad de la información que se procese, intercambie, reproduzca y conserve por medio de las tecnologías de información.

c) **Compartimentación**: Acción de dar a conocer lo que compete a cada persona, de acuerdo al acceso a la información oficial que le sea otorgado.

d) **Documento**: Cualquier objeto físico capaz de proporcionar información o datos que puedan ser transferidos del conocimiento de una persona a otra.

e) **Entidad**: Toda organización administrativa, comercial económica, productiva o de servicios de carácter estatal, cooperativa, privada o mixta, residente en el territorio nacional, así como las organizaciones sociales y de masas del país.

f) **OCIC**: Oficina para el Control de la Información Oficial Clasificada.

g) **Plan de Contingencia**: Documento básico contenido dentro del Plan de seguridad Informática, mediante el que se establecen medidas para restablecer y dar continuidad a los procesos informáticos ante una eventualidad o desastre.

h) **Plan de Evacuación, Conservación y Destrucción de la Información Oficial**: Documento básico que establece las medidas organizativas y funcionales para la evacuación, conservación o destrucción de la información oficial, que por sus características es necesario preservar o destruir al declararse una situación excepcional o producirse una catástrofe.

i) **Plan de seguridad Informática**: Documento básico que establece los principios organizativos y funcionales de la actividad de Seguridad informática en un órgano, organismo o entidad, a partir de las políticas y conjunto de medidas aprobadas sobre la base de los resultados obtenidos en el análisis de riesgo previamente realizado.

j) **Plan de Seguridad y Protección de la Información Oficial Clasificada**: Es el documento básico que establece el conjunto de medidas organizativas, administrativas, operativas, preventivas y de control dirigidas a garantizar la seguridad y protección de la información oficial clasificada e impedir su conocimiento u obtención por personas no autorizadas o por los servicios especiales extranjeros.

k) **Protección Criptográfica**: Proceso de transformación de información abierta en información cifrada mediante funciones, algoritmos matemáticos o sucesiones lógicas de instrucciones, con el objetivo de su protección ante personas sin acceso a ella.

l) **Seguridad Informática**: Conjunto de medidas administrativas, organizativas, físicas, técnicas, legales y educativas dirigidas a prevenir, detectar y responder a las acciones que

puedan poner en riesgo la confidencialidad, integridad y disponibilidad de la información que se procesa, intercambia, reproduce o conserva por medio de las tecnologías de información.

m) **Señalización**: acción de consignar de forma visible y expresa la categoría o término que le corresponde a la información oficial.

n) **Servicio Cifrado**: Actividad que se realiza mediante un conjunto de regulaciones, medidas organizativas y técnicas y medios de protección criptográfica de la información oficial clasificada que se tramita o almacena a través de las tecnologías de información.

o) **Tecnologías de Información**: Medios técnicos de computación o comunicación y sus soportes de información, que pueden ser empleados para el procesamiento, intercambio, reproducción o conservación de la información oficial.

CAPITULO II

DE LA AUTORIDAD COMPETENTE

ARTICULO 4.- El Ministerio del Interior es el organismo encargado de regular, dirigir y controlar la aplicación de la política del Estado y del Gobierno en cuanto a la Seguridad y Protección de la Información Oficial, y para el cumplimiento de estas funciones tienelas atribuciones siguientes:

a) dictar normas y procedimientos en materia de Seguridad y protección de la Información Oficial;

b) establecer los requisitos para elaborar los Planes de seguridad informática, de Contingencia, de Seguridad y Protección de la Información Oficial Clasificada y de Evacuación, Conservación y Destrucción de la Información Oficial para Situaciones Excepcionales y otras que puedan poner en riesgo la seguridad y protección de la información oficial;

c) certificar aquellas entidades que brinden servicio de seguridad Informática y criptográfica a terceros, así como la utilización, distribución o comercialización, de herramientas de Seguridad Informática.

d) regular y aprobar la producción de productos criptográficos, la aplicación de los Sistemas de Protección Criptográfica y la investigación y desarrollo científico en esta disciplina;

e) realizar inspecciones, auditorias y controles de la Seguridad y Protección a la Información oficial, incluyendo la Criptografía y la seguridad Informática;

f) promover la formación de personal calificado y el desarrollo de la ciencia y la tecnología en materia de Seguridad y Protección a la Información Oficial, la Seguridad Informática y la Criptografía;

g) realizar las acciones necesarias para cumplir y hacer cumplir los objetivos y funciones determinadas en el presente Decreto-Ley, tal y como se establece en el artículo 66 de la Constitución de la República de Cuba.

CAPITULO III

INFORMACION OFICIAL

ARTICULO 5.- La Información Oficial es aquella que posee un órgano, organismo, entidad u otra persona natural o jurídica residente en el territorio nacional o representaciones cubanas en el exterior, capaz de proporcionar directa o indirectamente datos o conocimientos que reflejen alguna actividad del Estado o reconocida por éste, y que pueda darse a conocer de cualquier forma perceptible por la vista, el oído o el tacto.

ARTICULO 5.1.- La Información Oficial constituye un bien del órgano, organismo, o entidad que la posea.

ARTICULO 6.- La Información Oficial, a los fines de establecer las medidas para su seguridad y protección, se divide en tres grupos:

a) CLASIFICADA
b) LIMITADA
c) ORDINARIA

SECCION PRIMERA

Información Oficial Clasificada

ARTICULO 7.- La Información Oficial Clasificada es la que posee un órgano, organismo, entidad u otra persona natural o jurídica, y que requiere de medidas de protección definidas por Ley, por contener datos o informaciones cuyo conocimiento o divulgación no autorizada puede ocasionar daños o entrañar riesgos para el Estado o para su desarrollo político, militar, económico, científico, cultural, social o de cualquier otro tipo.

ARTICULO 8.– La información Oficial Clasificada tiene las categorías de: SECRETO DE ESTADO, SECRETO Y CONFIDENCIAL.

ARTICULO 9.- La categoría SECRETO DE ESTADO es aquella cuyo conocimiento o divulgación no autorizada puede poner en peligro la seguridad, integridad, estabilidad o el funcionamiento del Estado.

ARTICULO 10.- La categoría SECRETO es aquella cuyo conocimiento o divulgación no autorizada puede causar perjuicios en las esferas política, militar, económica, científica, técnica, cultural, social o cualquier otra de importancia para el funcionamiento del estado.

ARTICULO 11.- La categoría CONFIDENCIAL es aquélla cuyo conocimiento o divulgación no autorizada puede ocasionar daños a la producción, los bienes, los servicios y en general a la gestión de cualquiera de ellos.

ARTICULO 12.- El tratamiento a la información oficial clasificada mediante tecnologías de información o de comunicación en las representaciones y delegaciones estatales fuera del territorio nacional se rige por medidas especiales de Protección Criptográfica y Seguridad Informática establecidas y controladas por el Ministerio del Interior.

ARTICULO 13.- Los cargos que requieren acceso a información oficial clasificada son determinados por el nivel de dirección administrativa facultada para ello.

ARTICULO 14.- El documento que contenga información oficial clasificada deberá tener la señalización de la categoría que le corresponda, según lo establecido en el Artículo 8.

ARTICULO 15.- Toda persona con acceso a información oficial clasificada mantendrá la debida compartimentación y se responsabilizará con protegerla y no divulgarla sin la autorización correspondiente.

ARTICULO 16.- La información oficial no puede ser modificada, alterada o destruida sin la debida autorización.

SECCION SEGUNDA

Información Oficial Limitada

ARTICULO 17.- La Información Oficial Limitada es aquella que sin poder ser conceptuada como clasificada, por su importancia o carácter sensible para el objeto social del órgano, organismo, o entidad u otra persona natural o jurídica que la posee, no resulta conveniente su difusión pública y debe limitarse su acceso a personas determinadas que no podrán destruirla, divulgarla ni modificarla sin la correspondiente autorización.

ARTICULO 18.- La Información Oficial Limitada se determina por el Jefe del órgano, organismo, entidad o persona natural o jurídica que la genera; se señala con el término LIMITADA, y se establecen medidas para su seguridad y protección.

ARTICULO 19.- Quien tenga acceso a información oficial limitada mantendrá la debida compartimentación y no podrá divulgarla sin la autorización correspondiente.

SECCION TERCERA

Información Oficial Ordinaria

ARTICULO 20.- La Información Oficial Ordinaria es aquella que posee un órgano, organismo o entidad, cuyo conocimiento o divulgación no autorizada no produce daños o riesgo para su funcionamiento.

CAPITULO IV

CLASIFICACION Y DESCALIFICACION DE LA INFORMACION OFICIAL

SECCION PRIMERA

De la clasificación y desclasificación

ARTICULO 21.- La Clasificación es el proceso mediante el cual se determina la categoría correspondiente a una información oficial, de acuerdo con el grado de afectación que su conocimiento o divulgación no autorizada pueda producir.

ARTICULO 22.- La Desclasificación es el proceso mediante el cual se le suprime la categoría de clasificación a una información oficial clasificada, al desaparecer los elementos que le dieron ese carácter.

SECCION SEGUNDA

Comisión Estatal para la Clasificación y Descalificación de la Información Oficial

ARTICULO 23.- Se crea la comisión Estatal para la Clasificación y Desclasificación de la Información Oficial, en lo adelante “la Comisión”, la cual elabora y somete a la aprobación del Comité Ejecutivo del Consejo de Ministros su Reglamento y la Lista general para la Clasificación y Desclasificación de la Información Oficial, así como ejecuta y controla los procesos para la clasificación de la información oficial.

ARTICULO 23.1.- Esta Comisión está presidida por el Ministerio del Interior e integrada además por un representante de cada órgano u organismo que ocupen cargos de dirección de Viceministros u otros equivalentes. Los representantes de la comisión tienen carácter permanente y son designados por el Jefe del órgano u organismo que representan.

SECCION TERCERA

Lista General para la Clasificación y desclasificación de la Información Oficial

ARTICULO 24.- La Lista General para la Clasificación y Desclasificación de la Información Oficial es el documento oficial donde se define el conjunto de asuntos considerados en la República de Cuba.

ARTICULO 25.- A la Lista General sólo tienen acceso los Jefes de los órganos, organismos o entidades del Estado y el personal autorizado por estos que por sus funciones así lo requieran.

ARTICULO 26.- Toda modificación que requiera efectuarse a la Lista General debe someterse a consulta de la comisión estatal para la clasificación y desclasificación de la información oficial, que la elevará al Comité Ejecutivo del consejo de Ministros para su aprobación.

SECCION CUARTA

Lista Interna para la Clasificación y Desclasificación de la Información Oficial

ARTICULO 27.- La Lista Interna para la Clasificación y Desclasificación de la Información Oficial es el documento oficial contentivo de las informaciones que se generan en cada órgano, organismo y entidad que constituyen asuntos definidos en la Lista General.

ARTICULO 28.- Cada órgano, organismo o entidad según corresponda elabora su lista Interna, la que es aprobada y puesta en vigor por Resolución u otra disposición del Jefe correspondiente.

ARTICULO 28.1.- A la Lista Interna tienen acceso los dirigentes, funcionarios y personal en general de los órganos, organismos y entidades que en atención a las funciones que realizan deben utilizar información oficial.

ARTICULO 29.- Toda modificación que se requiera efectuar a la Lista Interna, cuando afecte la Lista General, será sometida a consulta de la Comisión, que la elevará al Comité Ejecutivo del Consejo de Ministros para su aprobación.

CAPITULO V

RESPONSABILIDADES DE LOS ORGANOS, ORGANISMOS Y ENTIDADES

ARTICULO 30.- Los Jefes de órganos, organismos y entidades aseguran, controlan y exigen el cumplimiento de lo establecido en el sistema para la Seguridad y Protección de la Información Oficial.

ARTICULO 31.- Los Jefes de órganos, organismos y entidades en cada instancia están en la obligación de:

a) educar, preparar y concienciar al personal subordinado en mantener la debida discreción y compartimentación en cuanto a la Información Oficial Clasificada o Limitada que conozca en razón de su cargo, así como de cumplir todas las medidas que establezcan en materia de Seguridad y Protección de esta información;

b) ejercer especial control sobre el uso de los medios de computación portátil y soportes magnéticos, cámaras, casetes de video y televisión, rollos fotográficos, grabadoras y cintas fuera de los locales de trabajo, cuando contengan información oficial Clasificada o Limitada;

c) designar al personal que responde por la dirección, ejecución y control de la seguridad y protección de la Información Oficial Clasificada y Limitada;

d) designar una o más personas si se requiere con la idoneidad adecuada para que supervise y controle el cumplimiento de las medidas de Seguridad Informática y Criptográfica establecida en los lugares donde se procesa, intercambia, reproduce o conserva información oficial a través de las tecnologías de información;

e) garantizar que se proceda, ante la ocurrencia de hechos constitutivos de violaciones del sistema para la Seguridad y Protección de la Información Oficial Clasificada o Limitada, a la aplicación de las medidas correspondientes e informarlo de inmediato al órgano competente del Ministerio del Interior;

f) preparar al personal vinculado con la Seguridad y Protección a la Información Oficial y la Seguridad Informática;

g) aprobar los Planes de Seguridad Informática, de Contingencia, de Seguridad y Protección a la Información y de Evacuación, Conservación y Destrucción de la Información Oficial Clasificada y Limitada.

ARTICULO 32.- El Jefe de cada órgano, organismo o entidad, en correspondencia con el volumen de la Información Oficial clasificada, crea la Oficina para el Control de la Información Clasificada OCIC o designa la persona que se responsabiliza con la orientación y control del cumplimiento de las medidas para la seguridad y protección a esta información.

ARTICULO 33.- Los jefes de órganos, organismos o entidades en cada instancia, son los únicos facultados para autorizar al personal con acceso a la Información Oficial Clasificada o Limitada que le competa en cada momento, de acuerdo a las funciones que desempeña.

ARTICULO 34.- El Jefe es el único que puede autorizar dar a conocer información Oficial Clasificada generada en su órgano, organismo o entidad, procediendo de acuerdo a la categoría de clasificación que posea la misma.

ARTICULO 35.- Los Jefes de órganos, organismos o entidades, asegurarán que la Información Oficial Clasificada se trasmita con Protección Criptográfica, y decidirán cuando, por los riesgos que su conocimiento pueda producir, deba ser tratada en contactos personales exclusivamente.

ARTICULO 36.- Los dirigentes administrativos deben incluir en los planes económicos anuales y perspectivos los recursos financieros y materiales necesarios para la adquisición, instalación y mantenimiento de las medidas, medios técnicos y físicos requeridos para la Seguridad y Protección de la Información Oficial.

CAPITULO VI

PROTECCION CRIPTOGRAFICA

ARTICULO 37.- El Ministerio del Interior es el organismo encargado de representar al país en las relaciones de colaboración científica y tecnológica en la esfera de la Criptografía con países y organizaciones internacionales.

ARTICULO 38.- Es facultad del Ministerio del Interior autorizar la divulgación, promoción, elaboración de información, realización de eventos e intercambios de o sobre los sistemas de Protección Criptográfica. Los intereses que al respecto puedan presentarse serán coordinados y solucionados con dicho Ministerio.

ARTICULO 39.- Corresponde al Ministerio del Interior autorizar el diseño, producción, importación y comercialización de sistemas de protección criptográfica y prestación de estos servicios a órganos, organismos y entidades estatales.

ARTICULO 40.- Corresponde al Ministerio del Interior realizar las actividades de investigación y desarrollo para el diseño, producción, análisis, evaluación y aprobación de los Sistemas de Protección Criptográfica y los criptomateriales y de las aplicaciones criptográficas contenidas en los Sistemas Automatizados o de Comunicaciones.

ARTICULO 41.- La realización de estudios o investigaciones científicas y tecnológicas en interés de la Criptografía, por parte de personas naturales o jurídicas, se hará por necesidad y solicitud del Ministerio del Interior, o la iniciativa de aquellas, previa consulta y aprobación de dicho Ministerio, el que además certificará la aplicación, de todo Sistema de Protección Criptográfica.

ARTICULO 42.- El Ministerio del Interior es el organismo encargado de regular, dirigir y controlar el Servicio Central Cifrado Internacional del Estado y Gobierno Cubanos.

CAPITULO VII

SEGURIDAD INFORMATICA

ARTICULO 43.- En los órganos, organismos o entidades donde se procesa, intercambia, reproduce o conserva Información Oficial por medio de las tecnologías de información, se cumplirá las medidas que se requieran para su seguridad y protección, en correspondencia con las normas y regulaciones emitidas por el Ministerio del Interior.

ARTICULO 44.- Todos los órganos, organismos o entidades donde se procesa, intercambia, reproduce o conserva Información Oficial por medio de las tecnologías de información tienen que elaborar, aplicar y mantener actualizados permanentemente los Planes de Seguridad Informática y de Contingencia, acorde con lo establecido por el Ministerio de Interior para la seguridad informática y por el de la Industria Sidero Mecánica y la Electrónica para la seguridad técnica de los sistemas informáticos.

ARTICULO 45.- El Ministerio del Interior es el organismo competente para realizar Auditoria a la Seguridad Informática y el facultado para autorizar a otros órganos, organismos o entidades u otras personas naturales o jurídicas a realizarlas.

ARTICULO 46.- Se prohíbe procesar, reproducir o conservar Información Oficial clasificada con la categoría Secreto de Estado en las tecnologías de información conectadas en redes de datos.

ARTICULO 47.- Se prohíben las conductas que se describen a continuación:

a) Crear o diseminar programas malignos.

b) El acceso no autorizado a redes de datos.

c) Conectar tecnologías de información que procesen Información Oficial Clasificada a las redes de datos de alcance global.

ARTICULO 48.- La violación de lo establecido en los Artículo 46 y 47 será puesta en conocimiento de la autoridad administrativa que corresponda a los efectos de la aplicación de la medida que proceda, sin perjuicio de cualquier otra responsabilidad en que pudiere haberse incurrido.

ARTICULO 49.- En los órganos, organismos o entidades donde se procesa, intercambia, reproduce o conserva Información Oficial por medio de las tecnologías de información, se designa una o más personas en su caso, con su idoneidad requerida para que supervise y controle el cumplimiento de las medidas de Seguridad Informática establecidas.

CAPITULO VIII

PROTECCION ELECTROMAGNETICA

ARTICULO 50.- La Protección Electromagnética tiene como objetivo disminuir el riesgo que encierra las fugas de señales electromagnéticas contentivas de Información Oficial Clasificada o Limitada, emitidas por los Sistemas Informáticos durante su explotación. Comprende locales, medios y circuitos apantallados, sistemas de filtraje de señales, barreras técnicas y medidas complementarias.

ARTICULO 51.- Los Sistemas de Protección Electromagnética serán desarrollados y producidos en entidades nacionales autorizadas bajo el cumplimiento de normas y certificación emitidas por el Ministerio del Interior.

ARTICULO 52.- Las entidades que adquieran tecnologías de información por vías diferentes a las entidades nacionales autorizadas al efecto deberán, previo a su empleo, solicitar al Ministerio del Interior su homologación o certificación en relación con la Protección Electromagnética.

ARTICULO 53.- La aplicación de los sistemas de Protección Electromagnética en las entidades estará en correspondencia con los requerimientos de protección a la Información Oficial y de seguridad Informática.

DISPOSICIONES ESPECIALES

PRIMERA: Se faculta al Ministerio de las Fuerzas Armadas Revolucionarias para el desarrollo, reglamentación, aplicación y control de los Sistemas de Protección Criptográfica y de Seguridad Informática de uso propio.

SEGUNDA: El Ministerio del Interior presentará al Comité Ejecutivo del Consejo de Ministros, en un plazo de 180 días a partir de la fecha de aprobación del presente Decreto-Ley, la correspondiente propuesta para establecer el sistema de contravenciones en la materia que por éste se regula.

DISPOSICIONES FINALES

PRIMERA: Se faculta a los Ministerios de las Fuerzas Armadas Revolucionarias y del Interior, según corresponda, para adecuar en lo que resulte necesario, la aplicación de las disposiciones establecidas en este Decreto-Ley, en correspondencia con las particularidades de las funciones, misiones y características de la información de dichos organismos.

SEGUNDA: El Ministerio del Interior emitirá el Reglamento y demás disposiciones complementarias del presente Decreto-Ley en un plazo que no exceda los 90 días, contados a partir de la fecha de su aprobación y queda facultado para dictar cuantas otras disposiciones resulten necesarias para su mejor cumplimiento.

TERCERA: Se derogan la Ley número 1246 del Secreto Estatal del 14 de mayo de 1973 y el Decreto número 3753 del 17 de enero de 1974 que puso en vigor el Reglamento para la ejecución de la Ley del Secreto Estatal, así como el Decreto número 3787 del 23 de septiembre de 1974 que puso en vigor los Reglamentos gubernamentales para el Servicio Nacional y para el Servicio Cifrado Exterior; la Resolución del 25 de mayo de 1973 del Comandante en jefe en su condición de Primer Ministro, creando la Comisión Estatal para la Clasificación y Desclasificación de la Información, y cuantas disposiciones se opongan al cumplimiento del presente Decreto-Ley.

CUARTA: El Sistema para la Seguridad y Protección de la Información Oficial que se establece, comenzará a regir una vez transcurridos 180 días contados a partir de la publicación del presente Decreto-Ley en la Gaceta Oficial de la República.

DADO en el Palacio de la Revolución, en la ciudad de La Habana, a los 25 días del mes de noviembre de 1999.

Fidel Castro Ruz

Anexo 3- Acuerdo 6058/2007 de CECM

Primero: Aprobar los lineamientos para el perfeccionamiento de la seguridad de las tecnologías de la información en el país.

Segundo: El Ministerio de la Informática y las Comunicaciones implementará en el término de seis meses un reglamento de seguridad para las tecnologías de la información que responda a las necesidades actuales en esta materia, para su aplicación en todo el territorio nacional, así como las normas, regulaciones y procedimientos que se requieran para el cumplimiento de los presentes lineamientos.

Tercero: Los organismos de la Administración Central del Estado adoptarán las medidas necesarias para el fortalecimiento de la seguridad de las tecnologías de la información en sus respectivos sistemas en correspondencia con el esfuerzo que viene realizando el país en el desarrollo acelerado de la informática, para lo cual asegurarán, controlarán y exigirán en el ámbito de su competencia:

1. El establecimiento de niveles de seguridad informática apropiados.
2. La elaboración, aprobación, puesta en vigor y cumplimiento de los planes de seguridad informática y su permanente actualización.
3. La designación, preparación y control del personal responsabilizado por los sistemas informáticos y su seguridad.
4. Las acciones que se realicen mediante el empleo de las tecnologías de la información, particularmente aquellas que impliquen afectaciones a terceras partes.
5. Que las tecnologías y sistemas que se adquieran o se implementen garanticen el grado de seguridad requerido.
6. La implementación y ejecución de los procedimientos establecidos ante la ocurrencia de incidentes y violaciones de seguridad.

Cuarto: Los Consejos de Dirección de los órganos, organismos y entidades promoverán la observancia de la seguridad de las tecnologías de la información dentro de cada organización, para lo cual cumplirán lo siguiente:

1. La revisión y aprobación de las políticas de seguridad informática y las responsabilidades generales.
2. El monitoreo de cambios significativos en la exposición de los bienes informáticos a amenazas.
3. La revisión y el esclarecimiento de los incidentes de seguridad informática.
4. La aprobación de las iniciativas principales para incrementar la seguridad informática.
5. La evaluación de la idoneidad de los controles específicos de seguridad informática y la coordinación de su implementación para nuevos sistemas y servicios.

Quinto: Facultar al Ministerio de la Informática y las Comunicaciones para ejercer la inspección estatal a la seguridad de las tecnologías de la información y establecer las regulaciones correspondientes, así como las normas para la prestación de servicios de seguridad informática a terceros.

Sexto: El Ministro de la Informática y las Comunicaciones queda encargado de la ejecución de lo dispuesto en este acuerdo; así como, de mantener informada a la secretaría del comité ejecutivo del consejo de ministros a los efectos del control correspondiente.

Séptimo: Los ministerios de las Fuerzas Armadas Revolucionarias y del Interior, adecuarán y regularán para sus sistemas lo dispuesto en este acuerdo, de conformidad con sus estructuras y particularidades.

Y para publicar en la Gaceta Oficial de la República, remitir copias a los miembros del Comité Ejecutivo del Consejo de Ministros y a cuantos otros sea pertinente, se expide la presente certificación en el Palacio de la Revolución, a los 9 días del mes de julio de 2007, Año 49 de la Revolución.

Anexo 4- Reglamento de Seguridad para las tecnologías de la información

CAPITULO I

GENERALIDADES

Objetivos y Alcance

ARTÍCULO 1: El presente Reglamento tiene por objeto establecer los requerimientos que rigen la seguridad de las tecnologías de la información y garantizar un respaldo legal que responda a las condiciones y necesidades del proceso de informatización del país. Este Reglamento no sustituye las medidas específicas que norman el procesamiento de la información clasificada y limitada, que son objeto de normativas emitidas por el Ministerio del Interior.

ARTÍCULO 2: El término Seguridad de las Tecnologías de la Información utilizado en este Reglamento está relacionado con la confidencialidad, integridad y disponibilidad de la información tratada por los ordenadores y las redes de datos. El empleo de otros términos, tales como seguridad de la información, seguridad de los ordenadores, seguridad de datos o seguridad informática, tienen a los efectos de lo que aquí se establece, el mismo significado.

ARTÍCULO 3: Este Reglamento será de aplicación, en lo que a cada cual concierne, en todos los Órganos y Organismos de la Administración Central del Estado y sus dependencias; otras entidades estatales; empresas mixtas; sociedades y asociaciones económicas que se constituyan de acuerdo a la Ley; entidades privadas radicadas en el país; organizaciones políticas, sociales y de masas y personas naturales que posean o utilicen, en interés propio o de un tercero, tecnologías de la información. El cumplimiento de este Reglamento en áreas sensibles que son objeto de la atención directa del MININT y el MINFAR será realizado por los especialistas de estos órganos designados al efecto.

CAPITULO II

DEL SISTEMA DE SEGURIDAD INFORMATICA.

ARTÍCULO 4: Cada entidad que haga uso para el desempeño de su actividad de las tecnologías de la información está en la obligación de diseñar, implantar y mantener actualizado, un Sistema de Seguridad Informática a partir de la importancia de los bienes a proteger y de los riesgos a que están sometidos, con el fin de alcanzar los siguientes objetivos:

- Minimizar los riesgos sobre los sistemas informáticos.
- Garantizar la continuidad de los procesos informáticos.

ARTÍCULO 5: A partir del Sistema de Seguridad Informática diseñado, cada entidad elaborará su Plan de Seguridad Informática.

ARTÍCULO 6: El diseño del Sistema de Seguridad Informática y la elaboración del Plan de Seguridad Informática de cada entidad se realizarán en correspondencia con las metodologías establecidas al respecto por la Oficina de Seguridad para las Redes Informáticas, adscripta al Ministerio de la Informática y las Comunicaciones.

ARTÍCULO 7: Los jefes de entidades responden por la actualización de los Planes de Seguridad Informática, considerando para ello los siguientes factores:

a) La aparición de nuevas vulnerabilidades.

b) Los efectos de los cambios de tecnología o de personal.

c) La efectividad del sistema, demostrada por la naturaleza, número y daño ocasionado por los incidentes de seguridad registrados;

ARTÍCULO 8: En los Órganos y Organismos de la Administración Central del Estado y en aquellas organizaciones en que las tecnologías de la información son determinantes para su gestión se dispondrá de los cargos de especialistas de Seguridad Informática que se requieran para atender esta actividad, los cuales tendrán las siguientes atribuciones y funciones:

a) Organizar y controlar la actividad de Seguridad Informática.

b) Evaluar el estado de cumplimiento y aplicación de la base legal vigente en la materia.

c) Supervisar el trabajo del personal que responde por la Seguridad Informática en las entidades y organizar su preparación.

d) Proponer medidas ante violaciones de la base legal establecida en la materia.

ARTÍCULO 9: Los jefes a las diferentes instancias en los órganos, organismos y entidades responden por la protección de los bienes informáticos que le han sido asignados y tienen las siguientes obligaciones:

a) Identificar los requerimientos de seguridad de los bienes informáticos bajo su responsabilidad y de las aplicaciones en desarrollo, determinar el nivel de acceso de los usuarios a los mismos y la vigencia de estos accesos.

b) Participar en el diseño del Sistema de Seguridad y en la elaboración, evaluación y actualización del Plan de Seguridad Informática en la parte que concierne a su esfera de acción y garantizar su cumplimiento.

c) Aplicar las medidas y procedimientos establecidos en su área de responsabilidad.

d) Especificar al personal subordinado las medidas y procedimientos establecidos y controlar su cumplimiento.

e) Participar en la elaboración de los procedimientos de recuperación ante incidentes de seguridad y en sus pruebas periódicas.

f) Imponer o proponer sanciones ante violaciones del Sistema de Seguridad, en correspondencia con su naturaleza y con los daños ocasionados.

ARTÍCULO 10: El responsable de la actividad informática en cada entidad tiene las siguientes obligaciones:

a) Participar en el diseño del Sistema de Seguridad y en la elaboración, evaluación y actualización del Plan de Seguridad Informática, supervisar su aplicación y disciplina de cumplimiento.

b) Establecer y mantener los controles en correspondencia con el grado de protección requerido por el Sistema de Seguridad Informática diseñado.

c) Garantizar la disponibilidad de los bienes informáticos.

d) Asesorar a las distintas instancias sobre los aspectos técnicos vinculados con la seguridad de las tecnologías de la información.

e) Establecer los controles necesarios para impedir la instalación de cualquier tipo de hardware o software sin la autorización de la Dirección de la Entidad.

f) Participar en la elaboración de los procedimientos de recuperación ante incidentes de seguridad y en sus pruebas periódicas.

g) Informar a los usuarios de las regulaciones establecidas.

ARTÍCULO 11: Los usuarios de las tecnologías de la información asumen en primera instancia la responsabilidad de las consecuencias que se deriven de la utilización impropia de las mismas.

ARTÍCULO 12: Los usuarios de las tecnologías de información en órganos, organismos y entidades tienen las siguientes obligaciones:

a) Adquirir la preparación necesaria y los conocimientos de Seguridad Informática imprescindibles para el desempeño de su trabajo.

b) Contar con la autorización expresa del jefe facultado, para obtener acceso a cualquiera de los bienes informáticos.

c) Utilizar las tecnologías de información solo en interés de la entidad.

d) No transgredir ninguna de las medidas de seguridad establecidas.

e) Proteger las tecnologías o la terminal de red que le ha sido asignada y colaborar en la protección de cualquier otra, para evitar que sea robada o dañada, usada la información que contiene o utilizado de manera impropia el sistema al que esté conectada.

f) No instalar ni utilizar en las tecnologías equipamientos o programas ni modificar la configuración de las mismas, sin la correspondiente autorización del jefe facultado.

g) Cumplir las reglas establecidas para el empleo de las contraseñas.

h) Informar al dirigente facultado de cualquier anomalía de seguridad detectada.

CAPITULO III

EMPLEO CONVENIENTE Y SEGURO DE LAS TECNOLOGÍAS DE LA INFORMACION

Sección Primera- Clasificación y control de bienes informáticos

ARTÍCULO 13: Los bienes informáticos de una entidad deben ser utilizados en las funciones propias del trabajo en correspondencia con su objeto social.

ARTÍCULO 14: Todos los bienes informáticos de una entidad deberán estar identificados y controlados, para lo cual se conformará y mantendrá actualizado un inventario de éstos incluyendo sus componentes y las especificaciones técnicas de aquellos que pudieran ser suplantados.

ARTÍCULO 15: Cada uno de los bienes informáticos de una entidad tienen que ser puestos bajo la custodia documentada legalmente de una persona, que actuando por delegación de la dirección de la entidad, es responsable de su protección.

ARTÍCULO 16: Los jefes de entidades instrumentarán los procedimientos que se requieran para garantizar la autorización y el control sobre el movimiento de los bienes informáticos, los cuales deberán ser considerados a esos efectos de igual forma que el resto de los medios de la entidad.

Sección Segunda- Del personal

ARTÍCULO 17: Las funciones y responsabilidades de seguridad, tanto general como específica, serán documentadas y se incluirán dentro de las responsabilidades laborales del personal.

ARTÍCULO 18: El personal previsto para ocupar cargos vinculados a la actividad informática en órganos, organismos, entidades, organizaciones políticas, sociales y de masas, incluyendo personal eventual, estudiantes insertados y otros casos similares con acceso a sistemas críticos, a información de valor o a la supervisión y seguridad de los sistemas, deberá ser seleccionado adecuadamente.

ARTÍCULO 19: Los términos y condiciones del contrato de empleo incluirán la obligación de la entidad contratante en cuanto a la preparación del contratado, así como la responsabilidad del trabajador hacia la Seguridad Informática, precisando que este último aspecto mantiene su vigencia una vez finalizada la relación laboral. Deberán incluirse las acciones a tomar en caso que el trabajador pase por alto los requerimientos de seguridad.

ARTÍCULO 20: La utilización de las tecnologías y sus servicios asociados en cada entidad estará aprobada previamente por la dirección de la misma y basada en cada caso en la necesidad de uso por interés de la propia entidad.

ARTÍCULO 21: El uso no autorizado de las tecnologías de información y sus servicios asociados constituye una violación de los derechos de la entidad que es sancionable. Es un deber y un derecho de la dirección de cada entidad la supervisión del empleo de las tecnologías de la información por parte de los usuarios.

ARTÍCULO 22: Los Jefes a cada nivel, garantizarán que el personal vinculado a las tecnologías de la información esté capacitado para la utilización de las mismas, así como que conozca sus deberes y derechos en relación con el Sistema de Seguridad Informática implementado, los cuales deberán firmar una declaración como constancia de su conocimiento y compromiso de cumplimiento, que se incluirá en el contrato de trabajo.

ARTÍCULO 23: El acceso a las facilidades de procesamiento y a los servicios que brindan las tecnologías por parte de personal que no forme parte de la plantilla será en todos los casos objeto de una estricta autorización y control por parte de la dirección de cada entidad y a partir de los riesgos que esto pueda introducir se establecerán los requerimientos específicos que correspondan para garantizar la seguridad.

ARTÍCULO 24: Los usuarios de las tecnologías de la información están en la obligación de informar de inmediato cualquier incidente de seguridad, debilidad o amenaza a sistemas o servicios y las direcciones correspondientes exigirán su cumplimiento.

ARTÍCULO 25: Constituye una violación grave de la seguridad la realización de acciones de comprobación de vulnerabilidades contra sistemas informáticos nacionales o extranjeros.

ARTÍCULO 26: Ninguna persona está autorizada a introducir, ejecutar, distribuir o conservar en los medios de cómputo programas que puedan ser utilizados para comprobar, monitorear o transgredir la seguridad, así como información contraria al interés social, la moral y las buenas costumbres, excepto aquellas aplicaciones destinadas a la comprobación del sistema instalado en la organización para uso por especialistas expresamente autorizados por la dirección de la misma. En ningún caso este tipo de programas o información se expondrá mediante las tecnologías para su libre acceso.

Sección Tercera-Seguridad Física y Ambiental

ARTÍCULO 27: La dirección de cada entidad determinará las tecnologías de información que por las funciones a que estén destinadas, la información que contengan y las condiciones de los locales en que se encuentren ubicadas, requieran la aplicación específica de medidas de protección física.

ARTÍCULO 28: Las tecnologías de la información se ubicarán en áreas que garanticen la aplicación de medidas alternativas que permitan la creación de una barrera de protección a estos medios e impidan su empleo para cometer acciones malintencionadas o delictivas.

ARTÍCULO 29: En los edificios e instalaciones de cada entidad se determinarán áreas o zonas controladas con requerimientos específicos, protegidas por un perímetro de seguridad definido en dependencia de la importancia de los bienes informáticos contenidos en ellas y su utilización, de acuerdo con los criterios y denominaciones siguientes:

a) **Áreas limitadas,** son aquellas donde se concentran bienes informáticos de valor medio cuya afectación puede determinar parcialmente los resultados de la gestión de la entidad o de terceros.

b) **Áreas restringidas,** son aquellas en que se concentran bienes informáticos de alto valor e importancia crítica cuya afectación pueda paralizar o afectar severamente la gestión de ramas o sectores de la economía o de la sociedad; territorios o entidades.

c) **Áreas estratégicas**, son aquellas en que se concentran bienes informáticos de alto valor e importancia crítica que inciden de forma determinante en la seguridad y la defensa nacional; la seguridad aeronáutica; biológica; industrial; la generación y distribución de energía eléctrica; las redes informáticas y de comunicaciones del país; las relaciones exteriores y de colaboración; la economía nacional; las investigaciones científicas y el desarrollo tecnológico; la alimentación de la población; la salud pública y el suministro de agua.

ARTÍCULO 30: Las áreas o zonas controladas estarán protegidas con medidas adecuadas para garantizar el acceso exclusivamente al personal autorizado.

ARTÍCULO 31: La selección y diseño de las áreas controladas tomará en cuenta la posibilidad de daño por fuego, inundación, explosión, perturbaciones del orden y otras formas de desastre natural o artificial.

ARTÍCULO 32: El equipamiento instalado en las áreas controladas estará protegido contra fallas de alimentación y otras anomalías eléctricas, incluyendo el uso de fuentes de alimentación alternativas para los procesos que deban continuar en caso de un fallo de electricidad prolongado y será ubicado y protegido de manera tal que se reduzcan los riesgos de amenazas ambientales y oportunidades de cualquier tipo de acceso no autorizado.

ARTÍCULO 33: En las Áreas Limitadas se aplicarán las medidas de protección física siguientes:

a) Se ubicarán en locales cuyas puertas y ventanas estén provistas de cierres seguros;

b) A los locales que tengan ventanas que se comuniquen con el exterior de la instalación, se le aplicarán medidas que garanticen su seguridad y que eviten la visibilidad hacia el interior del mismo;

c) Se prohíbe el acceso de personal no autorizado por la dirección de la entidad.

d) Se prohíbe la permanencia del personal fuera del horario laboral sin la debida justificación y autorización por escrito de la dirección de la entidad. Las autorizaciones referidas serán conservadas para su verificación en caso de necesidad.

ARTÍCULO 34: En las Áreas Restringidas, además de las medidas requeridas en las Áreas Limitadas, se aplicarán las siguientes:

a) Tienen que permanecer cerradas, incluso cuando existan personas laborando en ellas, y el acceso a las mismas debe ser controlado mediante los documentos de registro que para ello se establezcan;

b) El personal que acceda a estas áreas deberá cumplir requisitos especiales de idoneidad.

c) Los medios informáticos no podrán estar conectados de manera física o lógica a medios que se encuentren fuera del alcance de estas áreas ni a redes públicas de transmisión de datos;

d) Se aplicarán sistemas de detección y alarma que permitan una respuesta , efectiva ante accesos no autorizados cuando no se encuentre el personal que labora en las mismas;

e) Se implementarán mecanismos y procedimientos de supervisión de la actividad que se realiza en estas áreas;

f) Se prohíbe la introducción de soportes ópticos y magnéticos personales, excepto los que hayan sido autorizados de forma expresa por la dirección de la entidad.

g) Se prohíbe la introducción de cámaras fotográficas, de grabación de imágenes o cualquier tipo de almacenamiento digital ajeno a la misma.

ARTÍCULO 35: En las Áreas Estratégicas, además de las medidas requeridas en las Áreas Restringidas y Limitadas, se aplicarán las siguientes:

a) Todo el personal que labora en ellas o que por razones de servicio sea autorizado a permanecer en las mismas, deberá contar con una identificación personal visible que distinga el área.

b) Se implementarán medios especiales de supervisión de la actividad que en ellas se realiza;

c) El acceso a estas áreas por personas ajenas a la misma solo se realizará de manera excepcional, restringida y bajo supervisión, mediante un permiso especial en cada caso emitido por la dirección de la entidad.

ARTÍCULO 36: Todas las tecnologías de información, independientemente de su importancia, se protegerán contra alteraciones o sustracciones, ya sea de éstas o sus componentes, así como de la información que contienen.

ARTÍCULO 37: En las redes de las entidades los cables de alimentación o de comunicaciones que transporten datos o apoyen los servicios de información se protegerán contra la intercepción o el daño. Los cables de alimentación deberán estar separados de los cables de comunicaciones para evitar la interferencia.

ARTÍCULO 38: Los jefes de entidades garantizarán que el equipamiento reciba el mantenimiento correcto de acuerdo con los intervalos de servicio y especificaciones recomendados por el fabricante para asegurar su disponibilidad e integridad continuas. En caso de necesidad de envío de equipamiento fuera de las instalaciones para que reciban mantenimiento, se realizará en

correspondencia con los procedimientos que se establezcan previamente para ello, observando las regulaciones establecidas en el país en materia de protección a la información.

ARTÍCULO 39: El uso fuera de las instalaciones de una entidad de cualquier equipo para el procesamiento de información tiene que estar autorizado legalmente por la dirección de la misma mediante el documento correspondiente. La seguridad que se le garantice deberá ser equivalente a la que tiene en las instalaciones habituales el equipamiento usado para el mismo propósito, tomando en cuenta los riesgos de trabajar fuera de la instalación.

ARTÍCULO 40: El equipamiento que cause baja o sea destinado para otras funciones será objeto de un procedimiento adecuado para evitar que la información que contiene pueda resultar comprometida. Los dispositivos de almacenamiento que contengan información crítica para la entidad deberán destruirse físicamente o sobrescribirse mediante un proceso completo en lugar de borrarlos como usualmente se hace.

ARTÍCULO 41: Se prohíbe el movimiento sin autorización de los equipos, la información o el software y en caso de que se autorice será realizado mediante un documento oficial que demuestre su legalidad y el movimiento deberá registrarse a la salida y a la entrada al reintegrarse el medio a su origen. Se deberán realizar inspecciones sorpresivas para detectar las extracciones no autorizadas.

Sección Cuarta-Seguridad de Operaciones

ARTÍCULO 42: Al determinar las responsabilidades que se asignan al personal se tendrá en cuenta el principio de separación de funciones, considerando aquellas tareas que no deben ser realizadas por una misma persona, a fin de reducir oportunidades de modificación no autorizada o mal uso de los sistemas informáticos.

ARTÍCULO 43: La introducción en una entidad de nuevos sistemas informáticos, actualizaciones y nuevas versiones será aprobada previamente a partir de su correspondencia con el sistema de seguridad establecido y los resultados de las pruebas que se realicen para determinar si cumple los criterios de seguridad apropiados.

ARTÍCULO 44: Las acciones para cubrir las brechas de seguridad y la corrección de los errores del sistema deberán estar minuciosamente controladas en cada entidad. Los procedimientos deberán asegurar que:

a) solo el personal claramente identificado y autorizado tenga acceso a sistemas en funcionamiento y a los datos;

b) todas las acciones de emergencia tomadas sean documentadas detalladamente;

c) la acción de emergencia sea reportada a la dirección y realizada de manera ordenada;

Sección Quinta-Identificación, autenticación y control de accesos

ARTÍCULO 45: En los sistemas en que es posible el acceso por múltiples usuarios se dispondrá para cada uno de ellos de un identificador de usuario personal y único. Las personas a las que se asignen identificadores de usuarios responden por las acciones que con ellos se realicen.

ARTÍCULO 46: La asignación de nuevos identificadores de usuarios en los sistemas se realizará a partir de un procedimiento que incluya la notificación del jefe inmediato del usuario. En caso de

terminación de la necesidad del uso de los sistemas por el cese de la relación laboral u otras causas, se procederá de forma análoga para la eliminación del identificador de usuario.

ARTÍCULO 47: Para la utilización de contraseñas como método de autenticación de usuarios, se cumplirán los siguientes requisitos:

a) Serán privadas e intransferibles.
b) Su estructura, fortaleza y frecuencia de cambio estarán en correspondencia con el riesgo estimado para el acceso que protegen.
c) Combinarán en todos los casos letras y números sin un significado evidente, con una longitud mínima de 6 caracteres.
d) No pueden ser visualizadas en pantalla mientras se teclean.
e) No pueden ser almacenadas en texto claro (sin cifrar) en ningún tipo de tecnologías de información.

ARTÍCULO 48: En cada entidad se definirán de manera estricta los derechos y privilegios de acceso a sistemas y datos que tiene cada usuario y se implementará un procedimiento escrito en cada caso para otorgar o suspender dichos accesos.

Sección Sexta-Seguridad ante programas malignos

ARTÍCULO 49: Se prohíbe el diseño, la distribución o intercambio de códigos de virus informáticos u otros programas malignos entre personas naturales o jurídicas; se exceptúa la información enviada por usuarios a la autoridad competente para el análisis e investigación de programas malignos.

ARTÍCULO 50: En cada entidad se implementarán los controles y procedimientos para protegerse contra virus y otros programas dañinos que puedan afectar los sistemas en explotación, así como para impedir su generalización. Para la protección contra virus se utilizarán los programas antivirus de producción nacional u otros autorizados oficialmente para su uso en el país, debidamente actualizados.

ARTÍCULO 51: Ante indicios de contaminación por programas malignos, tanto en redes como en equipos no conectados a redes, se procederá al cese de la operación de los medios implicados y a su desconexión de las redes cuando corresponda, preservándolos para su posterior análisis y descontaminación por personal especializado y se revisarán los soportes con los cuales haya interactuado el medio contaminado.

ARTÍCULO 52: La contaminación por virus informáticos u otros programas malignos se considera un incidente de seguridad y se cumplirá en este caso lo establecido en el Artículo 89 del presente Reglamento. En todos los casos se determinará el origen y la responsabilidad de las personas involucradas.

Sección Séptima-Respaldo de la información

ARTÍCULO 53: Todas las entidades están en la obligación de implementar un sistema fiable de respaldo de la información esencial para su funcionamiento que permita la recuperación después de un ataque informático, desastre o fallo de los medios, para lo cual ejecutarán los procedimientos que aseguren la obtención sistemática de las copias que se requieran.

ARTÍCULO 54: La información de respaldo, conjuntamente con informes precisos y completos de las copias de respaldo y los procedimientos de recuperación documentados deberán almacenarse en otra ubicación que le permita no afectarse en caso de desastre en la ubicación principal.

ARTÍCULO 55: La información de respaldo deberá tener una protección física y ambiental consecuente con las normas aplicadas en la ubicación principal. Los controles aplicados a los medios en la ubicación principal deberán extenderse a la ubicación de los medios de respaldo.

ARTÍCULO 56: Los medios de respaldo deberán probarse regularmente y verificar su estado de actualización con el fin de asegurar que pueda confiarse en ellos para un uso de emergencia cuando sea necesario.

Sección Octava-Seguridad en Redes

ARTÍCULO 57: Los órganos, organismos y entidades están en la obligación de implementar los mecanismos de seguridad de los cuales están provistas las redes, así como de aquellos que permitan filtrar o depurar la información que se intercambie.

ARTÍCULO 58: En todas las redes se habilitarán las opciones de seguridad con que cuentan los sistemas operativos de forma tal que se garantice la protección de los servidores y las terminales, el acceso a la información solamente por personal autorizado y los elementos que permitan el monitoreo y auditoria de los principales eventos por un tiempo no menor de un año.

ARTÍCULO 59: Para la fiscalización y el monitoreo del empleo que se le da a las redes de datos y de los servicios en ellas implementadas las entidades instalarán los productos autorizados en el país para esos propósitos.

ARTÍCULO 60: La arquitectura y la configuración de los diferentes componentes de seguridad de una red y la implementación de sus servicios estarán en correspondencia con las políticas definidas y aprobadas para su empleo y en ningún caso deben ser el resultado de la iniciativa de una persona con independencia de la preparación que ésta posea.

ARTÍCULO 61: Toda red de computadoras deberá contar para su operación con la existencia de al menos una persona encargada de su administración.

ARTÍCULO 62: El Administrador de una red tiene, en relación con la Seguridad Informática, las siguientes obligaciones:

a) Garantizar la aplicación de mecanismos que implementen las políticas de seguridad definidas en la red.

b) Realizar el análisis sistemático de los registros de auditoria que proporciona el sistema operativo de la red.

c) Garantizar que los servicios implementados sean utilizados para los fines que fueron creados.

d) Comunicar a la dirección de la entidad los nuevos controles técnicos que estén disponibles y cualquier violación o anomalía detectada en los existentes.

h) Activar los mecanismos técnicos y organizativos de respuesta ante los distintos tipos de incidentes y acciones nocivas que se identifiquen, preservando toda la información requerida para su esclarecimiento.

i) Participar en la elaboración de los procedimientos de recuperación ante incidentes y en sus pruebas periódicas.

e) Informar a los usuarios de las regulaciones de seguridad establecidas y controlar su cumplimiento.

f) Participar en la confección y actualización del Plan de Seguridad Informática.

ARTÍCULO 63: La gestión de administración de las redes implica la concesión de máximos privilegios, debiéndose realizar directamente desde los puestos de trabajo habilitados al efecto. Se prohíbe la administración remota de estas redes mediante conexiones conmutadas a través de las redes públicas de transmisión de datos.

ARTÍCULO 64: Se prohíbe la adición de algún equipo o la introducción de cualquier tipo de software en una red, ya sea a través de soportes removibles o mediante acceso a redes externas, sin la autorización de la dirección de la entidad, garantizando su compatibilización con las medidas de seguridad establecidas para la protección de dicha red.

ARTÍCULO 65: Los usuarios que han recibido la autorización para el empleo de los servicios que brindan las redes son responsables por su propia conducta. Los usuarios deben conocer las políticas de seguridad para las computadoras y redes a que ellos acceden y están en la obligación de cumplir estas políticas.

ARTÍCULO 66: En las redes que prevean conexiones desde o hacia el exterior de una entidad es obligatorio instalar los medios técnicos que aseguren una barrera de protección entre las tecnologías de información de la entidad y la red externa, mediante los mecanismos de seguridad que sea necesario implementar.

ARTÍCULO 67: Las entidades instrumentarán la ejecución de procedimientos periódicos de verificación de la seguridad de las redes con el fin de detectar posibles vulnerabilidades, incluyendo para ello cuando sea procedente la comprobación de forma remota por entidades autorizadas oficialmente a esos efectos, debido a la sensibilidad de estas acciones.

ARTÍCULO 68: Las entidades autorizadas oficialmente para la comprobación de la seguridad de las redes de otras entidades están en la obligación de:

a) Garantizar la profesionalidad que requiere esta actividad.

b) Obtener la aprobación previa de las entidades que requieren estos servicios para su realización.

c) Mantener el máximo de discreción con relación a las posibles vulnerabilidades detectadas.

d) Abstenerse de la utilización del conocimiento obtenido sobre la red comprobada en beneficio propio.

e) Informar a la Oficina de Seguridad para las Redes Informáticas de los resultados de las comprobaciones realizadas.

ARTÍCULO 69: En las redes donde se establezcan servicios de intercambio de datos o mensajes con otras redes o usuarios externos se implementarán mecanismos de seguridad que garanticen la confidencialidad, la integridad, el control de accesos, la autenticación y el no repudio, según corresponda.

ARTÍCULO 70: Las entidades que coloquen información en servidores para su acceso público, establecerán las medidas y procedimientos que garanticen su integridad y disponibilidad, así como la correspondencia de su contenido con los intereses de la propia entidad y del país.

ARTÍCULO 71: Si por necesidades de conectividad u otros intereses se requiere hospedar un sitio en servidores ubicados en un país extranjero, siempre se hará como espejo o réplica del sitio principal en servidores ubicados en Cuba, estableciendo las medidas requeridas para garantizar su seguridad, particularmente durante el proceso de actualización de la información.

ARTÍCULO 72: Se prohíbe la colocación de páginas o sitios Web desde entidades estatales en servidores extranjeros que ofrecen estos servicios de forma gratuita.

ARTÍCULO 73: Los servidores de redes de una entidad destinados a facilitar accesos hacia o desde el exterior de las mismas no serán instalados en las máquinas en que se instalen los servidores destinados para el uso interno de dicha red.

ARTÍCULO 74: En los casos de redes corporativas que prevean la extrapolación de servicios internos, esto se realizará por puertos bien identificados y mediante la protección con dispositivos que garanticen el acceso a esos servicios por el personal autorizado.

ARTÍCULO 75: Los servicios que ofrecen las redes de datos de una entidad mediante conexiones externas solo se utilizarán en interés de la misma. La asignación de cuentas para el empleo de estos servicios será aprobada en todos los casos por la dirección de la entidad sobre la base de las necesidades requeridas para su funcionamiento.

ARTÍCULO 76: Se prohíbe el establecimiento de cuentas de correo electrónico desde entidades estatales en servidores que se encuentran en el exterior del país, considerando la inseguridad que el empleo de los mismos implica para la entidad por hallarse fuera del control del Estado Cubano. Si de manera excepcional por no haber otra alternativa, surgiera esta necesidad de forma puntual, tiene que ser aprobada previamente y por escrito por la dirección de la entidad, a partir de la valoración de las razones existentes, especificando claramente el tipo de información que se va a transmitir y el plazo de vigencia de esta modalidad.

ARTÍCULO 77: Se prohíbe vincular cuentas de correo electrónico de un servidor de una entidad a un servidor en el exterior del país con el fin de redireccionar y acceder a los mensajes a través del mismo.

ARTÍCULO 78: La suscripción a listas de correo electrónico y el empleo de servicios de conversación en tiempo real (chat) por parte del personal de una entidad será autorizado en todos los casos por la dirección de la misma en correspondencia con sus intereses y de las normas particulares establecidas para estos servicios, debiendo documentarse esta autorización de manera que pueda ser objeto de comprobación.

ARTÍCULO 79: Se prohíbe la difusión a través de las redes públicas de transmisión de datos de información contraria al interés social, la moral, las buenas costumbres y la integridad de las personas; o que lesione la Seguridad Nacional, por cualquier persona natural o jurídica. Las entidades instalarán los controles y mecanismos que permitan detectar y obstaculizar este tipo de actividades. Las violaciones detectadas serán informadas oportunamente a las instancias pertinentes.

ARTÍCULO 80: Ninguna persona natural o jurídica está autorizada para enviar mensajes de correo electrónico no solicitados a múltiples usuarios de forma indiscriminada (spam), ya sean de carácter informativo, comercial, cultural, social, con intenciones de engaño (hoax) u otros.

ARTÍCULO 81: Las redes proveedoras de servicios tomarán las medidas que se requieran para impedir la sobrecarga de los canales de comunicaciones, restringiendo el envío o recepción de grandes volúmenes de información y la generación de mensajes a múltiples destinatarios.

ARTÍCULO 82: Las entidades implementarán controles dirigidos a impedir e interrumpir la generación de cartas en cadena y el envío de mensajes de correo de forma masiva a través de las redes.

ARTÍCULO 83: Las entidades con redes destinadas a proveer servicios a otras personas naturales o jurídicas mediante conexiones remotas están en la obligación de cumplir los aspectos siguientes:

a) Establecer las medidas y procedimientos de Seguridad Informática que garanticen la protección de los servicios a brindar y los intereses de seguridad de los que los reciben.
b) Implementar los mecanismos y procedimientos que aseguren la identificación del origen de las conexiones, incluidas las conmutadas, así como su registro y conservación por un tiempo no menor de un año.
c) Dar a conocer a los clientes de estos servicios los requerimientos de Seguridad Informática que deben cumplir en correspondencia con las políticas de seguridad establecidas en la red que los brinda.
d) Facilitar el acceso de las autoridades competentes a los registros de las conexiones y cooperar con las mismas en la investigación de violaciones de las normas establecidas y de incidentes de seguridad.

ARTÍCULO 84: Ninguna persona, natural o jurídica está autorizada para explorar o monitorear las redes públicas de transmisión de datos en busca de vulnerabilidades o información sobre los usuarios legales de las mismas.

ARTÍCULO 85: El acceso no autorizado o la agresión a cualquier sistema de cómputo conectado a las redes públicas de transmisión de datos y la usurpación de los derechos de acceso de usuarios debidamente autorizados se consideran violaciones del presente Reglamento, independientemente de otras implicaciones legales que puedan derivarse de estas acciones.

CAPITULO IV

GESTIÓN DE INCIDENTES DE SEGURIDAD

ARTÍCULO 86: Las entidades están obligadas a formular la estrategia a seguir ante cualquier incidente o violación de la seguridad que pueda producirse en correspondencia con la importancia de los bienes informáticos que posea y las posibles alternativas a emplear para garantizar los servicios. Dicha estrategia deberá ser consecuente con los objetivos básicos de la entidad y tomará en consideración:

a) Los riesgos que la entidad enfrenta en términos de su probabilidad y su impacto, incluyendo una identificación y asignación de prioridades a los procesos críticos.

b) El impacto probable de las interrupciones sobre la gestión de la entidad.

c) Comprobar y actualizar regularmente los planes y procesos establecidos.

ARTÍCULO 87: Una vez establecida la estrategia a seguir, las entidades dispondrán las medidas y procedimientos que correspondan con el fin de garantizar la continuidad, el restablecimiento y la recuperación de los procesos informáticos.

ARTÍCULO 88: Las medidas y procedimientos de recuperación serán definidas a partir de la identificación de los posibles eventos que puedan causar la interrupción o afectación de los procesos informáticos e incluirán las acciones de respuesta a realizar, la determinación de los responsables de su cumplimiento y los recursos necesarios en cada caso.

ARTÍCULO 89: Los procedimientos para la gestión de incidentes y violaciones de Seguridad Informática, especificarán los pasos a seguir para garantizar una correcta evaluación de lo que ha ocurrido, a quién, cómo y cuándo debe ser reportado, la respuesta adecuada, así como los aspectos relacionados con su documentación, la preservación de las evidencias y las acciones a seguir una vez restablecida la situación inicial. Para ello considerarán lo siguiente:

a) el reporte inmediato de la acción a la autoridad correspondiente;

b) la comunicación con los afectados o los involucrados en la recuperación del incidente;

c) el análisis y la identificación de las causas de los incidentes;

d) el registro de todos los eventos vinculados con el incidente;

e) la recolección y preservación de las trazas de auditoría y otras evidencias;

f) la planificación y la implementación de medidas para prevenir la recurrencia, si fuera necesario;

ARTÍCULO 90: Ante cualquier incidente que afecte la Seguridad Informática de una entidad, se designará por la dirección de la misma una comisión presidida por un miembro del Consejo de Dirección e integrada por especialistas no comprometidos directamente con el incidente, que realizará las investigaciones necesarias con el fin de esclarecer lo ocurrido, determinar el impacto, precisar los responsables y proponer la conducta a seguir.

ARTÍCULO 91: La dirección de cada entidad garantizará que al producirse un incidente o violación de la seguridad informática la información sobre este acontecimiento se reporte inmediatamente a la Oficina de Seguridad para las Redes Informáticas y a la instancia superior de la entidad. Este reporte incluirá como mínimo:

a) En que consistió el incidente o violación.
b) Fecha y hora de comienzo del incidente y de su detección.
c) Implicaciones y daños para la entidad y para terceros.
d) Acciones iniciales tomadas.
e) Evaluación preliminar

CAPITULO V

PRESTACIÓN DE SERVICIOS DE SEGURIDAD INFORMÁTICA A TERCEROS.

ARTÍCULO 92: Solo estarán autorizadas a brindar servicios de Seguridad Informática a terceros aquellas entidades que cuenten con la correspondiente autorización emitida por la Oficina de Seguridad para las Redes Informáticas, adscripta al Ministerio de la Informática y las

Comunicaciones.

ARTÍCULO 93: Los requerimientos que debe cumplir una entidad para solicitar la autorización para prestar servicios de Seguridad Informática a terceros son los siguientes:

a) que el objeto social de dicha entidad coincida con estos fines;

b) que dicha entidad cuente con mecanismos que garanticen la calidad de los servicios y la idoneidad del personal;

c) preparación técnico - profesional de los especialistas que laboren en la entidad;

d) que la entidad esté en condiciones de cumplir los reglamentos y disposiciones establecidos en esta materia;

e) que cuente con medios de protección de la información a la que tenga acceso durante su trabajo;

f) que los productos de Seguridad Informática, que utilicen estén debidamente certificados por los órganos correspondientes del Ministerio de la Informática y las Comunicaciones; y

g) que el capital sea enteramente nacional y el personal designado para brindar los servicios sea ciudadano cubano y resida de forma permanente en el país.

CAPITULO VI

DE LA INSPECCION A LA SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACION

ARTÍCULO 94: El Ministerio de la Informática y las Comunicaciones tiene como atribución estatal la ejecución de inspecciones en materia de Seguridad a las Tecnologías de la Información.

ARTÍCULO 95: La inspección estatal en esta materia será ejecutada exclusivamente por los inspectores del Ministerio de la Informática y las Comunicaciones.

ARTÍCULO 96: Los Jefes de Órganos, Organismos y Entidades facultarán a especialistas debidamente preparados para realizar controles en materia de Seguridad Informática en las entidades subordinadas.

Sección Primera-Objetivos

ARTÍCULO 97: La inspección estatal a la Seguridad a las Tecnologías de la Información tiene los objetivos siguientes:

a) Evaluar los conocimientos y la aplicación de la base legal vigente.

b) Realizar diagnósticos sobre la efectividad de los Sistemas de Seguridad Informática aplicados en las entidades.

c) Verificar el grado de control y supervisión que se ejerce sobre los bienes informáticos, así como los resultados de la gestión de la Seguridad Informática.

d) Valorar la efectividad de los Planes de Seguridad Informática elaborados y su actualización y correspondencia con las necesidades de cada entidad.

e) Valorar la gestión e influencia que ejercen las instancias superiores sobre esta actividad.

Sección Segunda-Facultades de los inspectores

ARTÍCULO 98: Los inspectores de Seguridad Informática tienen las facultades siguientes:

a) Realizar la inspección con aviso previo o sin él.
b) Evaluar el estado del cumplimiento y aplicación de la base legal de Seguridad Informática vigente.
c) Identificar las violaciones y vulnerabilidades detectadas en el Sistema de Seguridad Informática.
d) Hacer evaluaciones, recomendaciones y disponer acciones correctivas ante violaciones de la base legal establecida.
e) Proponer sanciones administrativas u otra de las previstas en el Artículo 99.
f) Recomendar la realización de auditorias.
g) Proponer la suspensión de los servicios cuando se viole lo establecido en el presente Reglamento.
h) Verificar el cumplimiento de las acciones correctivas que hayan sido aplicadas como resultado de inspecciones anteriores si las hubiere.
i) Exigir la entrega de las trazas o registros de auditoria de las tecnologías de la información u otras posibles evidencias que se consideren necesarias.
j) Ocupar para su revisión los medios informáticos involucrados en cualquier tipo de incidente de seguridad y proponer su decomiso definitivo a las instancias correspondientes.

CAPITULO VII

DE LOS INCUMPLIMIENTOS

ARTÍCULO 99: Toda persona natural o jurídica que incumpla lo dispuesto en la presente Resolución y en las disposiciones legales vigentes en la materia, estará sujeta a la aplicación de las siguientes medidas:

a) Invalidación temporal o definitiva de las autorizaciones administrativamente concedidas por el Ministerio de la Informática y las Comunicaciones al infractor, entre ellas, cancelación de licencias, permisos, autorizaciones, desconexión parcial o total de las redes privadas de datos y otras;

b) Suspensión y/o cancelación, temporal o definitiva, de los servicios de informática y comunicaciones que hayan suscrito con empresas debidamente reconocidas y autorizadas por el Estado cubano;

d) Ocupación cautelar de los medios, instrumentos, equipamientos y otros utilizados para cometer la infracción, con la finalidad de disponer posteriormente el decomiso de los mismos, según proceda.

e) La aplicación de las medidas que correspondan, de conformidad con lo legalmente establecido.

ARTÍCULO 100: Toda persona natural o jurídica sujeta a la aplicación de las medidas descritas anteriormente puede apelar ante el Ministro del Ministerio de la Informática y las Comunicaciones en el plazo de 30 días hábiles contados a partir de la fecha de aplicada la medida. A su vez el Ministro dispondrá de 90 días hábiles para dar respuesta a dicha reclamación. La decisión de esta última instancia será inapelable.

Anexo 5- El Cibercomando de los EUA

El Cibercomando de Estados Unidos (USCYBERCOM) es un comando subunificado de las Fuerzas Armadas de Estados Unidos bajo el mando del Comando Estratégico de Estados Unidos y fue creado por el Secretario de Defensa de Estados Unidos Robert Gates el 23 de Junio de 2009. El comando está dirigido por el General Keith B. Alexander, y asumirá la responsabilidad de diversas agencias ya existentes. La capacidad operacional inicial fue alcanzada el 21 de Mayo de 2009 y su cuartel general se encuentra en Fort Meade, Maryland. Tenía planeada su plena operatividad a partir del 1 de octubre de 2010, pero anunciaron que esto no era posible porque no habían logrado completar la plantilla de 1 000 hackers que necesitan.

Sus antecesoras la Fuerza de Tarea Conjunta de Operaciones de Red Global (JTF-GNO) y el Comando Conjunto de Componentes Funcionales para la Guerra de red (JFCC-NW) debieron ser disueltas en octubre de 2010. La Agencia de Defensa de Sistemas de Información, donde hasta ahora operaba el JTF-GNO, prestará asistencia técnica y la garantía de la información al USCYBERCOM.

Como misión, "el USCYBERCOM planea, coordina, integra, sincroniza y conduce actividades para: dirigir las operaciones y defender las redes de información especificadas por el Departamento de Defensa y; prepararse para, cuando sea oportuno, llevar a cabo una amplia variedad de operaciones militares en el ciberespacio a fin de llevar a cabo acciones en todos los dominios, asegurar la libertad de acciones a los Estados Unidos y sus aliados en el ciberespacio y impedir lo mismo a nuestros adversarios"[164]. El texto "9ec4c12949a4f31474f299058ce2b22a", que se encuentra inscrito en el anillo interior del emblema del comando, es la encriptación de dicha misión.

Con USCYBERCOM se fusiona un abanico de operaciones del Departamento de Defensa en el ciberespacio y planeará, coordinará, integrará, sincronizará y llevará a cabo las actividades para: liderar la defensa diaria y proteger las redes de información del Departamento de Defensa, coordinar las operaciones del Departamento de apoyo a las misiones militares, dirigir operaciones y defensa de redes de información especificadas por el Departamento de Defensa y; prepararse para, cuando sea oportuno, llevar a cabo una gran variedad de operaciones militares ciberespaciales. El comando se encargará de agrupar los recursos ciberespaciales existentes, creando una sinergia que no existía anteriormente.

En Mayo de 2010, el General Keith Alexander esbozó su punto de vista en un informe para el Comité de los Servicios Armados del Congreso, donde expresaba: "*Mi punto de vista es que el único camino para contrarrestar tanto el espionaje como las actividades criminales en la red es siendo proactivos. Si los Estados Unidos están tomando una aproximación formal a este asunto, es algo bueno. Los chinos son la principal fuente de la mayoría de los ataques de las infraestructuras del Occidente y recientemente, del sistema de suministro eléctrico de Estados*

[164] U.S. Department of Defense, Cyber Command Fact Sheet, May 21, 2010 http://www.stratcom.mil/factsheets/cc/

Unidos. Si se determina que esto fue un ataque organizado, me gustaría eliminar el origen de esos ataques. El único problema es que Internet, por su naturaleza, no tiene fronteras y si los Estados Unidos asume el mando de la policía mundial, esto no podría funcionar tan bien."

En respuesta a las preocupaciones sobre los derechos de los militares a responder a ciberataques, el General Alexander declaró que "*Los Estados Unidos deben devolver el fuego a los ciberatacantes rápida y fuertemente y deben actuar para contrarrestar o inhabilitar una amenaza aunque la identidad del atacante sea desconocida*."[165]

"*El nuevo Cibercomando de Estados Unidos necesita alcanzar un equilibrio entre la protección de activos militares y privacidad personal… Este comando no trata sobre el esfuerzo de militarizar el ciberespacio, más bien, es sobre salvaguardar nuestros activos militares* " declaró Alexander, en un comunicado del Departamento de Defensa.[166]

La creación del Cibercomando de Estados Unidos parece haber motivado a otros países en este tema. En diciembre de 2009, Corea del Sur anunció la creación de un Comando de Guerra Cibernética, y la agencia de inteligencia británica GCHQ ha iniciado la preparación de una ciber-fuerza. El actual interés por la guerra informática en varias naciones ha motivado la creación del primer Centro de Inteligencia de Ciberguerra en Estados Unidos.

Estados Unidos ha creado además el primer Centro de Inteligencia de Ciberguerra de Estados Unidos, un superlaboratorio ubicado en Utah al cual se destinaron 1,2 mil millones de dólares, que será como una super CIA global, con información recopilada por EEUU y sus aliados.

[165] http://www.washingtonpost.com/wp-dyn/content/article/2010/03/18/AR2010031805464.html
[166] http://www.defense.gov/News/NewsArticle.aspx?ID=58772

Anexo 6- Los 10 servicios de redes sociales más populares en el 2010[167]

10.-Orkut

Orkut es promovida por Google desde enero del 2004. Tiene 34 millones de usuarios.

La red está diseñada para permitir a sus integrantes mantener sus relaciones existentes y hacer nuevos amigos, contactos comerciales o relaciones más íntimas. Aquí es posible crear y mantener comunidades, que agrupan personas de acuerdo a sus gustos e intereses, en diferentes categorías, entre las que se cuentan: actividades, negocios, juegos, música, mascotas, religión, escuelas, comidas, preferencias sexuales, y algunas más.

Hasta hace algún tiempo solo podían acceder a esta comunidad aquellos que recibían una invitación de alguien que ya pertenecía a ella, esto mientras el servicio permanecía en fase beta. Hoy está abierta a cualquier persona, para ello es necesario tener una cuenta de e-mail simplemente.

El servicio ha sido diseñado por el actual empleado turco de Google Orkut Büyükkökten quien, para su anterior empleador Affinity Engines ya había creado un sistema similar denominado "InCircle" y cuyo objetivo eran las comunidades de alumnos universitarios.

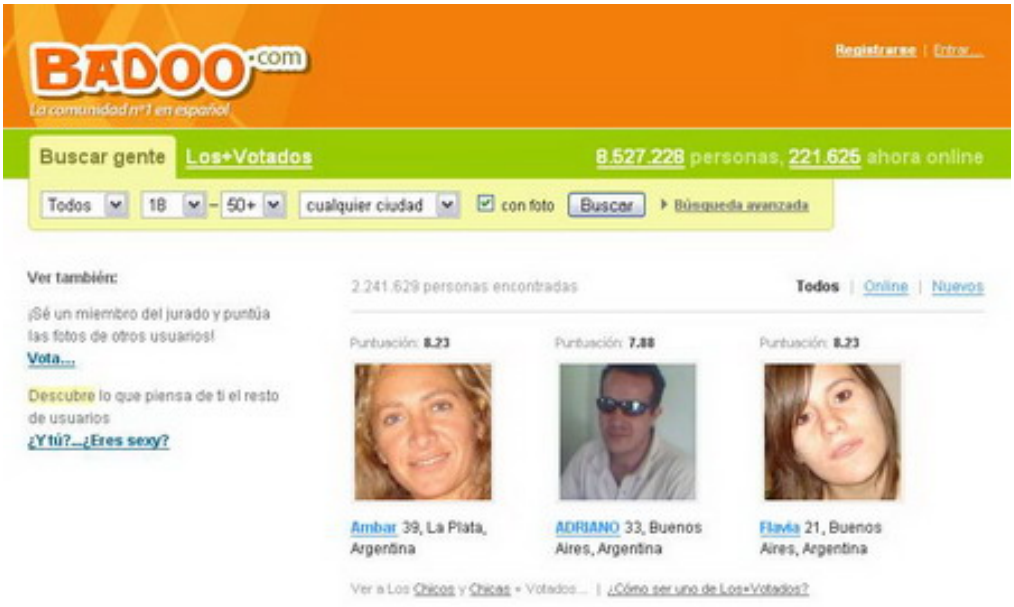
En junio de 2004 Affinity Engines demandó a Google, debido a que consideran que Orkut está basado en el código fuente de InCircle. La acusación se basa en que algunos errores presentes en InCircle también están presentes en Orkut.

En sus inicios fue una red anglófona, mayoritariamente de EE.UU.. Sin embargo, desde el 2004 hasta el día de hoy, sus visitantes se han ido polarizando en 2 países: Brasil, que han ido creciendo exponencialmente y supera el 49.5% del total de visitas y India con un 35.8%.

También destaca la mayoría de gente entre los 13-25 años (superior al 50%), usado para contactar con amigos por una amplia mayoría (superior al 80%) y el estado de soltería (con alrededor de un 40%).

[167] http://www.scribd.com/doc/36381805/LAS-10-REDES-SOCIALES-MAS-POPULARES-DEL-2010

9.-Badoo



Badoo es una popular plataforma de encuentros, creada en Gran Bretaña. Tiene más de 20 millones de usuarios.

Permite que los usuarios se comuniquen y permanezcan en contacto a través de mensajes, fotos y videos, pero además, está diseñado para que las personas se promocionen a sí mismos y puedan conquistar audiencias.

Badoo fue creado en Londres, en el 2006. Está entre las 100 páginas más visitada en el mundo.

Registrarse en Badoo es gratuito, basta con un correo y hay que rellenar un formulario con la información requerida por la página. Una vez registrado, el usuario tiene su propio perfil. En el perfil, se puede poner una foto de presentación y habrá muchas preguntas sobre información personal que el usuario. Cada persona puede decidir qué nivel de privacidad desea tener. Puede permitir que su perfil sea visto por todos los usuarios o sólo por los amigos.

8.-Metroflog

MetroFlog es un servicio de blogs fotográficos o fotoblogs en idioma español. Fue creado en Buenos Aires, Argentina, y posee más de 70 millones de usuarios.

Es popular sobre todo entre adolescentes y accesible para cualquier persona que cuente con una dirección de e-mail e Internet.

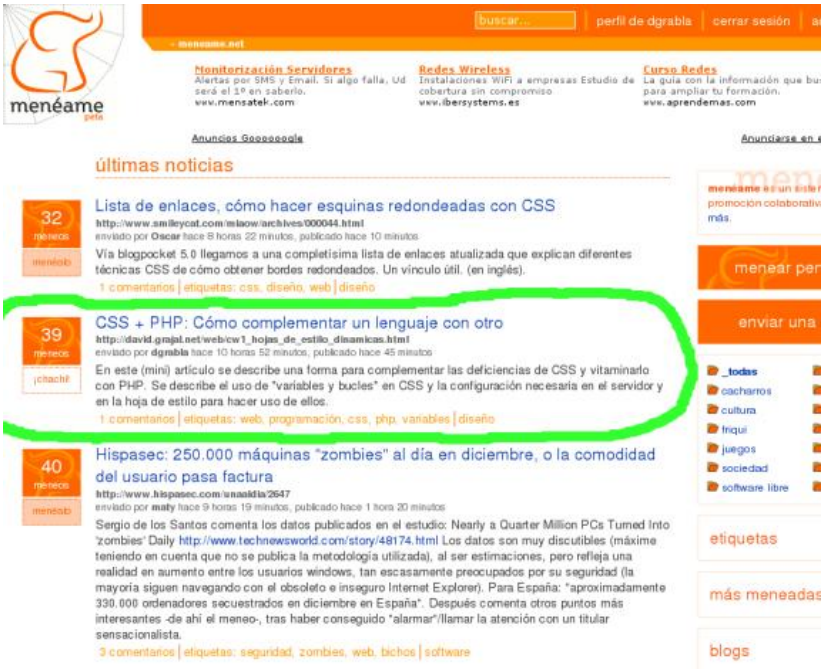
Según Alexa Internet, está entre las 100 páginas web más

visitadas del mundo (puesto 681 el 24 de septiembre de 2008), la mayoría desde Latinoamérica (principalmente México). Según este mismo ranking, en septiembre de 2008 llegó a superar a Fotolog.com, sitio en el que está basado su sistema de publicación de fotografías.

Permite agregar links, contenidos, enlaces, música, videos… En julio de 2009 se ha agregado un servicio denominado "muro" en el cual los usuarios pueden comunicar lo que están haciendo en cada momento.

En general, lo que los miembros de MetroFlog buscan es la "popularidad", aumentando la cantidad de "favoritos" y así el límite para agregar imágenes se expande y la cantidad de fotos que el usuario puede subir por día crece.

7.-Menéame



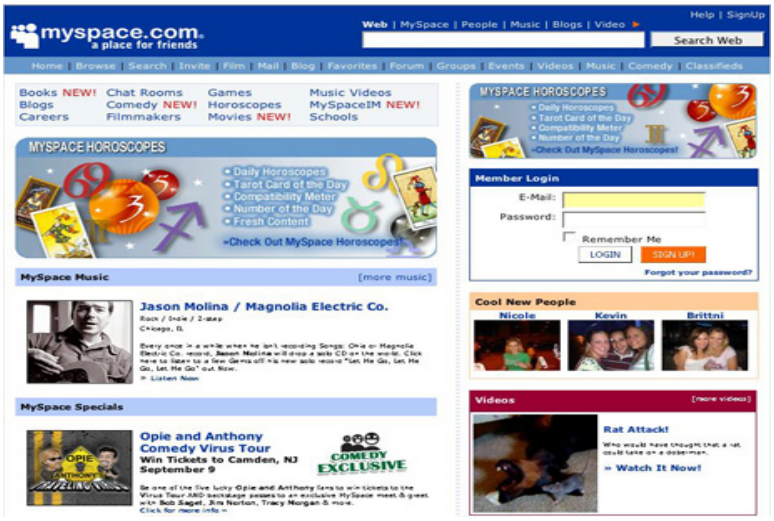
Menéame es un sitio web basado en la participación comunitaria en el que los usuarios registrados envían historias que los demás usuarios del sitio (registrados o no) pueden votar, promoviendo las más votadas a la página principal aunque con un claro control por parte del web. Tiene dos millones de visitantes cada mes y 150 000 usuarios registrados.

Como el modelo anglosajón en que se inspira (Digg), combina marcadores sociales, el blogging y la sindicación con un sistema de publicación sin editores.

Es un proyecto personal de Ricardo Galli, profesor del departamento de informática de la Universidad de las Islas Baleares, y Benjamí Villoslada, que además colabora en todo lo que respecta al aspecto e imagen del sitio web y asuntos legales o financieros. Fue desarrollado desde cero a finales del año 2005, hecho público el 7 de diciembre de 2005 y liberado como software libre bajo la licencia Affero GPL el 12 de diciembre de 2005.

Entre las motivaciones para crear Menéame, según su autor, estuvo el darle a la blogosfera hispana una herramienta equivalente al Digg estadounidense, pero que, a diferencia de éste, fuera software libre, para que cualquiera pudiera usar el código para crear su propia versión del sitio.

6.-MySpace



MySpace es un espacio de interacción social constituido por perfiles personales de usuarios que incluye redes de amigos, grupos, blogs, fotos, vídeos y música, además de una red interna de mensajería que permite comunicarse a unos usuarios con otros y un buscador interno. Tiene 95 millones de usuarios.

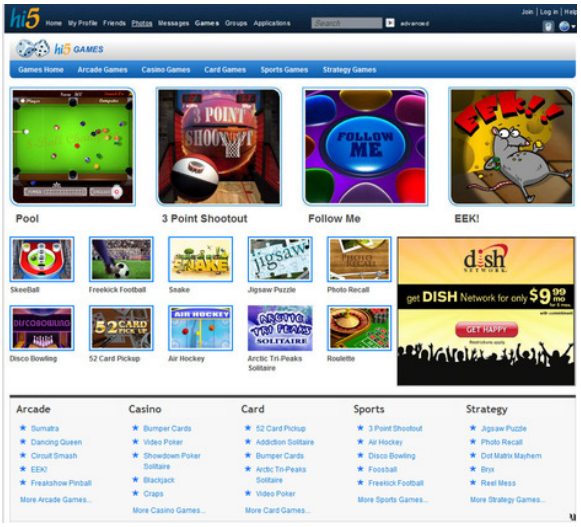
Fue creado por Tom Anderson, Chris DeWolfe y un grupo de programadores. En julio del 2005 fue adquirido por la "News corporation", cuenta con 300 empleados, con 200.623.371 usuarios (en septiembre de 2007) y su velocidad de crecimiento es de unos 230.000 usuarios al día. Su sede central se encuentra en California, Estados Unidos y además tiene otra sede y servidor en la ciudad de Nueva York, Estados Unidos. Según el sitio web Alexa dedicado a medir el tráfico de Internet, MySpace es el decimosegundo sitio más visitado de toda la red2 y el cuarto sitio más visitado de la red de lengua inglesa; aunque por otro lado, este sitio es poco frecuentado en Australia.

MySpace comenzó a expandirse y ganar popularidad además de usuarios lentamente, hasta llegar al punto de convertirse en algo fuera de lo común y en una revolución social, especialmente en Estados Unidos donde MySpace es el sitio web más visitado tras Yahoo!, MSN, Google y YouTube y hasta el punto en el que la mayoría de la población del país conoce el servicio y es muy habitual, especialmente entre jóvenes y adolescentes estadounidenses, ser usuario de MySpace. En la actualidad el servicio se está extendiendo mundialmente y ganando usuarios de otros países.

Entre sus posibilidades, MySpace ofrece perfiles especiales para músicos y sus usuarios usan el servicio con diversos y diferentes fines, entre ellos el comunicarse con amigos o familiares, el conocer gente, por motivos de trabajo, como ha servido para que grupos musicales se den a conocer, así todos tienen un perfil en la página, siendo a veces más visitada que la verdadera página oficial. En Latinoamérica y España la barrera del idioma ha impedido hasta ahora que se extienda su uso, aunque ya existe una versión beta del web en castellano.3

En mayo de 2007, myspace compra el sitio photobucket. En abril de 2008, se lanza un servicio de música streaming por suscripcion4

5.-Hi5



Es una plataforma de uso muy simple, creada para obtener un medio por el cual conectarse socialmente en línea con muchas personas. Con el tiempo fue evolucionando para agradar más a los usuarios y agregando nuevas aplicaciones, impulsado además por la aparición de fuertes competidores.

La página ha logrado posicionarse como una de las redes sociales más populares, con más de 50 millones de visitantes mensuales y 90 millones de usuarios registrados. Está disponible en 37 idiomas.

Fue fundada por Ramun Yalamanchis (actual director general de la empresa hi5 Networks) y que fue lanzada en el 2003. Ya tiene más de 90 millones de usuarios registrados, la mayoría de ellos en América Latina; además, es uno de los 40 sitios web más visitados del mundo.

Registrarse en Hi5 es muy fácil. Lo importante es tener un correo electrónico y luego llenar los datos paso por paso. Una vez registrado, uno dispone de una página personal o perfil en el que se pueden realizar muchas cosas y agregar aplicaciones.

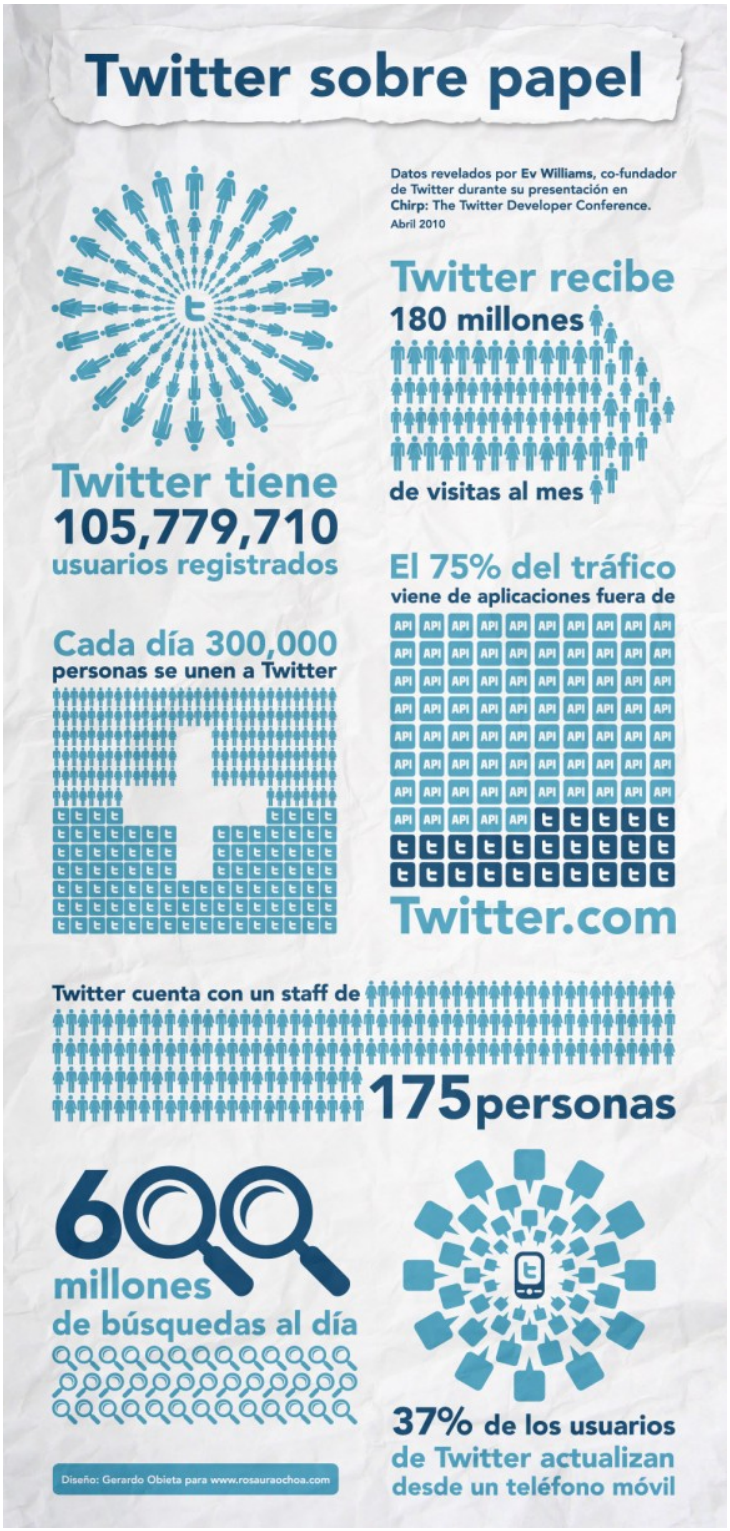
Hi5 es como una presentación personal, por lo que se pueden escribir datos o información personal que uno desee que los demás puedan conocer. Además, el usuario elige los colores que desea y así personalizarla al máximo. Como cualquier otro usuario registrado puede leer la información expuesta, el dueño del perfil puede bloquear el acceso a su página y dejarla disponible sólo para sus amigos. La red de amigos puede ser ilimitada, pero uno puede elegir 15 amigos principales para estar conectados con ellos de manera más fácil.

4.-Yahoo Respuestas

Siempre que hacemos una consulta en cualquier buscador uno de los primeros resultados los tiene la Wikipedia, sin embargo otro servicio que salió de la nada y una gran apuesta de cientos de millones de dólares que hizo Yahoo a este proyecto, logró consolidarse como uno de los sitios web de "descubrimiento" si se puede decir así que hay.

Yahoo Answers permite hacer cualquier tipo de preguntas, según su categoría y cualquier otro usuario puede responder esta pregunta y así mismo otros pueden calificar y elegir la mejor respuesta.

3.-Twitter



Gráfica de enero de 2010

El nombre significa en inglés "gorjear". Es un sistema de microblog con textos de hasta 140 caracteres, menos que lo que suele enviarse por el servicio de mensajería corta para celular (SMS). Sirve para comentar "cualquier cosa". Permiten seguir agendas, calendarios o actividades del día. También, coberturas de hechos noticiosos, titulares de prensa, adelantos de ediciones y reportes continuos desde los lugares donde se producen las noticias. Tiene 140 millones de usuarios.

El envío de mensajes se puede realizar casi desde cualquier dispositivo conectado en Internet y se han desarrollado decenas de herramientas para "twitear". Estas actualizaciones se muestran en la página de perfil del usuario, y son también enviadas de forma inmediata a otros usuarios que han elegido la opción de recibirlas.

A estos usuarios se les puede restringir el envío de estos mensajes sólo a miembros de su círculo de amigos o permitir su acceso a todos los usuarios, que es la opción por defecto.

Los usuarios pueden recibir las actualizaciones desde la página de Twitter, vía mensajería instantánea, SMS, RSS y correo electrónico.

Twitter tiene convenio con unas 50 compañías de telecomunicaciones en el mundo, para permitir la actualización vía SMS, apuntando a un número gratuito de los usuarios de cada compañía. Ha habilitado lo que llama "un código largo", a través del cual se pueden enviar mensajes para ser publicado automáticamente en Twitter, a partir de un costoso mecanismo de verificación.

Nació en 2006 como proyecto de investigación. Fue la plataforma de lanzamiento de un campaña contra el gobierno iraní en el verano de 2009, presentado una gran oleada de mensajes contra el resultado de las elecciones en ese país. Business Week reconoció posteriormente que el 68 por ciento de los mensajes que se tuitearon se originaron en EEUU, y que de los 100 000 tuiteros que los enviaron, solo 100 estaban en Irán.

En abril de 2010, otre hecho sacudió esta plataforma: el registro del Presidente Chávez como usuario de Twitter, con la cuenta @chavezcandanga. Tiene más de 800 000 seguidores y derrumbó el mito de que estos espacios eran exclusivos de la derecha venezolana. (Más información en el anexo)

2.-Facebook

Facebook es considerada una de las redes sociales con mayor cantidad de usuarios activos en Internet. Tenía 598 millones de usuarios, en septiembre de 2010. Si fuera un país, Facebook sería el tercero más poblado del planeta, solo superado por China y la India.

Se creó en el 2004 en la universidad de Harvard, en Estados Unidos, cuando el estudiante Mark Zuckerberg, de veinte años en aquel momento, utilizó una página de intercambio de archivos para estudiantes de esa universidad. Luego se expandió a colegios de la Yvy League, y después a todos los estudiantes universitarios, y finalmente a todos los mayores de 13 años.

El registro en esta red es libre. Todo lo que se necesita es una cuenta de correo y una contraseña. Hay que rellenar una plantilla con el perfil de cada usuario, datos que después permiten asociar a cada individuos a grupos por edad, sexo, estudios, gustos, etc, una base de datos valiosísima para las empresas y los servicios de inteligencia.

Además de fotos y textos, también se pueden subir vídeos y compartir cientos de aplicaciones desarrolladas por terceros, que reproducen todo tipo de servicios virtuales. Los usuarios también pueden asociarse o crear grupos y proyectos, algunos de gran impacto político como el "No+FARC", creado según rumores por los servicios de inteligencia colombianos a inicios de 2008, y que logró articular manifestaciones en decenas de ciudades en el mundo, con más de un millón de participantes.

1.-YOUTUBE

Youtube se ha convertido en el segundo website en el mundo en número de búsquedas y cuenta con más de 350 millones de usuario únicos cada mes que ven 1.000 millones de vídeos al día. Cada minuto se suben 24 horas de vídeo a Youtube. Fue la plataforma de lanzamiento de la campaña de Barack Obama para la Presidencia de los Estados Unidos.

En YouTube los usuarios pueden subir y compartir vídeos. Fue creado por tres antiguos empleados de la empresa de software PayPal, en febrero de 2005: Chad Hurley, Steve Chen y Jawed Karim en febrero de 2005 en San Bruno, California.

Es muy popular gracias a la posibilidad de alojar vídeos personales de manera sencilla. Aloja una variedad de clips de películas, programas de televisión, vídeos musicales (a pesar de las reglas de YouTube contra subir vídeos con derechos de autor, este material existe en abundancia), así como contenidos amateur como videoblogs .

En noviembre de 2006 Google Inc. lo adquirió por 1650 millones de dólares, y ahora opera como una de sus filiales. YouTube usa un reproductor en línea basado en Adobe Flash para servir su contenido. En estos momentos se pueden subir videos de hasta 15 minutos y con un peso de hasta 2 Gb. Admite formatos de Alta Definición, tanto para computadoras como para celulares, y recientemente inauguró un servicio de transmisión en vivo.

Los enlaces a vídeos de YouTube pueden ser también puestos en blogs y sitios electrónicos personales usando sistemas automatizados o incrustando cierto código.

Anexo 7- Redes sociales: “Lo esencial sigue siendo tomar La Bastilla”

Tamara Roselló, Revista América en Movimiento, de la ALAI. Abril 2011

Rosa Miriam Elizalde recientemente obtuvo el premio *Juan Gualberto Gómez*, en periodismo digital (2010). Con este reconocimiento la Unión de Periodistas de Cuba distingue a profesionales de la prensa nacional por su trabajo anual. Desde una ventana digital la editora del sitio Cubadebate, sigue los sucesos más urgentes del mundo y de su propio país. Dialoga con otros cibernautas y estudia (y logra) una alternativa de comunicación que desde la izquierda, aprovecha las oportunidades de las redes sociales en internet, porque “para conocer este mundo hay que meterse en él, hay que usar esas herramientas de una manera crítica”, asegura. Delante de la computadora sigue los últimos sucesos en Japón tras el terremoto del 11 de marzo. Comparte informaciones con los seguidores de su sitio en Facebook y Twitter e invita al intercambio y al análisis de estos procesos tecnológicos que atraviesan cada vez más nuestras sociedades contemporáneas. **América en movimiento** suma algunas de sus reflexiones en ese ir y venir de la práctica a la teoría, un viaje al que dedica la mayor parte de su tiempo.

-Las movilizaciones en el Oriente Medio han recolocado los debates sobre el rol de las redes sociales en internet. ¿Cuánto ha contribuido este contexto a la mitificación o no de espacios como Facebook o Twitter?

-Hay una especie de evangelismo digital que trata de sobredimensionar la trascendencia de las redes sociales. Esta es una visión interesada y manipuladora, que intenta supeditar las motivaciones de los individuos a determinados instrumentos, que no son neutrales. Las redes sociales establecen entre los individuos lazos débiles, esenciales para compartir información y crear puentes entre subgrupos, **pero no determinan la voluntad de los usuarios para movilizarse en torno a una acción,** particularmente aquella en la que nos va a veces hasta la vida. Emplearse de lleno en algo así necesita de entornos y estructuras sociales con relaciones muy sólidas, como las que uno tiene con familiares y amigos cercanos. Tener 2 000 “amigos” en Facebook y otro tanto de “seguidores” en Twitter permite encontrar gente con intereses comunes e identificar un camino, como el que se muestra en los mapas, y en Túnez y Egipto estas asociaciones indicaron dónde quedaba la plaza para exigir la renuncia de los gobernantes, pero un mapa no es el paisaje real, no es la razón para sumarse a una protesta. Nada habría pasado sin la voluntad, la decisión de la gente de manifestarse y luchar por el cambio.

En otras palabras, **la tecnología por sí misma no crea revoluciones.** No lo creó ahora, ni lo hizo antes. A nadie se le ocurre hoy decir que le debemos la Revolución francesa a las octavillas o la Revolución rusa al telégrafo, los medios de la época, que obviamente fueron utilizados con eficacia por los revolucionarios franceses y rusos. Pero lo esencial sigue siendo la voluntad, ese impulso colectivo que llevó a miles de personas a tomar un buen día la Bastilla y asaltar el Palacio de Invierno.

-¿Por qué interesa esta percepción de las redes sociales como elemento catalizador de las protestas?

-El software social no es una red social, sino un instrumento que facilita la interacción entre los seres humanos. Decir que MySpace es una red social es como decirle agua al vaso que la contiene. Por tanto, el primer elemento manipulador es la misma semántica que se ha impuesto para identificar estos instrumentos, que son muchos y que gracias al escalamiento de las tecnologías cada vez responden mejor a las exigencias de la comunicación. Lo que conocemos

como “redes sociales” en Internet facilitan extraordinariamente esta nueva dimensión de la vida humana que se ha incorporado a lo que llamamos el “mundo real”, que hasta hace tres décadas solo se pensaba, fundamentalmente, en términos de la realidad física. Hoy lo real es el mundo físico y el mundo virtual.

Lo virtual no es una cosa extraña, todopoderosa, sino la expresión simbólica del mundo tal y cual existe, un reflejo. Es como si de pronto el ser humano adquiriera noción de que convive permanentemente con su sombra, una especie de Platón postmoderno. Solo en las películas las sombras son otra cosa que la proyección de un individuo concreto. De modo que decir que en cualquier lugar de este mundo un gobierno puede ser sustituido por Google, o que Twitter es el responsable de las movilizaciones contra este o aquel gobierno, es un disparate o peor, una mentira, que no puede repetirse sino malintencionadamente. Un ejemplo es la famosa “*Revolución verde iraní*“, del verano del 2009.

Los medios nos vendieron los acontecimientos en Irán como una protesta organizada a través de Twitter. La verdad salió a la luz tan rápido como había llegado la mentira -solo que muchos ni se enteraron-. Businessweek publicó unos datos reveladores: de los 10 000 tuiteros que participaron activamente en la “revuelta”, solo 100 estaban en territorio iraní. ¿Por qué Estados Unidos nos vendió esta farsa? Porque hoy es posible convencer a la gente de que un símbolo es la realidad, y una sombra es un país, y con este juego de sombras chinas Estados Unidos ha intervenido en los asuntos de las demás naciones o ha invadido a otros, cuando se le antoja.

Y la opinión pública tiene muy mala memoria. Sabemos que una mentira sirvió para invadir Iraq. Bueno, ¿y qué? Ya fue olvidada. Es lo único que explica que en tiempo récord, más rápido que cuando Saddam Hussein era el malo de la película, el Consejo de Seguridad de la ONU dominado por EEUU logró ese acuerdo contra Libia, que incluye la posibilidad de la intervención militar.

-¿Significa esto que hay que darle la espalda a las “redes sociales”?

-Claro que no. No tengo ninguna duda de que si José Martí viviera hoy fuera “feibucero” y “tuitero”. Son instrumentos y espacios de comunicación donde cada vez más están conviviendo las audiencias, particularmente los jóvenes. Facebook tiene más de 600 millones de individuos cautivos en su plataforma -el 80 por ciento son menores de 35 años- y Twitter, más de 200 millones de seguidores. Internet ya tiene más de 2 000 millones de usuarios y se espera que antes del 2015 la mitad de la población esté enlazada a la red.

No se pueden construir alternativas políticas ni crear puentes de comunicación al margen de estos espacios, que como te dije antes no son neutrales y hay que asumirlos críticamente, pero teniendo claro que son ineludibles. Son las nuevas plazas públicas, donde ya no funciona el paradigma de los *mass media* -un punto de emisión y muchos receptores “pasivos”-, sino que cada individuo es receptor y emisor gracias a estas tecnologías. El discurso unidireccional, el hombre hablando a una multitud encaramado en un cajón de bacalao, se acabó. No hay manera de entablar la comunicación ahora si no escuchas al otro, si no te integras a una comunidad y si no haces cosas con otros, es decir, si no cooperas.

-¿Qué desafíos tiene la contrainformación frente a este nuevo paradigma?

-A la izquierda aún le cuesta mucho trabajo entender este cambio de paradigma. Generalmente vemos dos actitudes frente a las llamadas redes sociales: la paranoica o la panglossiana. O le tememos o sobrevaloramos sus posibilidades. La única manera de que nuestros proyectos tengan expresión en el mundo real es conociendo a profundidad cómo interactúan en la sociedad

contemporánea las redes sociales y las redes tecnológicas, y solo a partir del conocimiento se pueden generar alternativas y construir espacios liberadores para los ciudadanos de este planeta, que viven en el Siglo XXI, con sus maravillas y sus iniquidades. No hay manera de sobrevivir ni política, ni económica, ni socialmente al margen de estas redes. Marginarse es suicida, tanto como asumir acríticamente todo lo que las transnacionales de las telecomunicaciones, esclavas de las políticas imperiales, han diseñado para reproducir las lógicas de un sistema injusto, excluyente, estupidizante, que nos ha convencido de que lo importante es lo interesante, que una sombra deformada de la realidad es la realidad.

Tenemos que aceptar el reto tecnológico, elaborar un pensamiento a partir de esta nueva realidad y, desde el punto de vista de la comunicación, convertir lo importante en interesante, sin hacer concesiones de principios, pero sin ignorar que la forma del mensaje, en un mundo donde lo simbólico tiene tanto peso, no es menos trascendente que el mensaje.

-WikiLeaks ha irrumpido en la red para traernos a todos noticias de las interioridades de esas estrategias de dominación que suelen enmascararse, ¿cómo podríamos aprovechar más el impulso que representa?

- WikiLeaks es un parte aguas, gústele o no al Imperio y a muchos compañeros nuestros, inobjetablemente revolucionarios, que también le han dado hasta con el cabo del hacha a Julian Assange, a sus colaboradores y a su plataforma. Nos guste más o menos el señor Assange con sus discurso anarquizoides y sus poses de estrella de rock, la realidad es que ha puesto en crisis el sistema totalitario de la mentira como arma de terror e intervención política y militar. Ningún poder mentiroso está a salvo, por muy sofisticados policías cibernéticos que posea.

De hecho, la verdadera ciberguerra no empezó entre los estados, como advertía el Pentágono para justificar su enorme ejército de hackers integrados en el Cibercomando, sino entre los gobiernos que nos imponen la palabra y la imagen únicas, como dice Eduardo Galeano, y el ciudadano común. Los valores del ser humano siguen decidiendo por encima de las tecnologías. La diferencia es que antes la gente no tenía wikis y ahora sí, y lo que tardaba años en saberse gracias al altruismo, la decencia y a veces la inmolación de algunos individuos, si es que se llegaba a saber, ahora puede ser revelado en el momento. Es una bomba atómica el habernos levantado un día sabiendo que cualquiera es Wikileaks y para ello basta con un celular, una memoria flash, un correo electrónico, un blog.

En el caso de las revelaciones de los documentos del Departamento de Estado, esto no pone en crisis ni al sistema imperial, ni a la oficina de Hillary Clinton, ni a su enorme aparato mediático y sus sofisticados controles de riesgo. Pero le resta una enorme credibilidad, es decir poder. Nunca habíamos visto a Estados Unidos tan histérico con filtraciones de documentos, hasta el punto de armar una cacería sin precedentes contra los desarrolladores de Wikileaks, amenazar de muerte a Julian Assange y tratar al soldado Bradley Manning peor que a los terroristas que tumbaron las Torres Gemelas. A mí, personalmente, me conmueve muchísimo lo que Manning le dijo por chat a un hackers que luego vendió la información que conduciría a este soldado de 22 años a la cárcel:

“Si tuvieses acceso sin precedentes a redes clasificadas durante 14 horas al día, 7 días a la semana durante más de 8 meses, ¿qué harías?… Te hablo de cosas increíbles, cosas horrorosas que deben pertenecer al dominio público y no a algún servidor almacenado en una oscura habitación en Washington”.

Esa pregunta se la han hecho muchos a lo largo de la historia y se la seguirán haciendo: qué haces frente al crimen, te conviertes en un cómplice o denuncias al criminal. Lo único nuevo aquí es, como dije antes, que la respuesta a esa pregunta puede tener consecuencias devastadoras e inmediatas para el poder criminal que se sostiene en la mentira.

-¿Cuál ha sido la lógica de la política y las estrategias de los EEUU con respecto a "las libertades en internet" y el ciberactivismo que han potenciado para la "democracia"?

Ha habido una adecuación del discurso del gobierno de EEUU, particularmente el de la llamada Diplomacia pública norteamericana. Empezando el 2010 una eufórica Hillary Clinton nos hablaba de "derrumbar la cortina de hierro de Internet" y anunciaba la inauguración de la "Diplomacia del Siglo XXI", cuyo objetivo número uno parecía ser iluminar los "oscuros rincones del planeta", para usar la frase de Bush, con la luz de "libertad" de Internet. Sin embargo, en enero de este año su discurso dedicado a la Red de Redes tuvo un tono más bien sombrío.

Para empezar ya no está tan segura de que se pueda exportar "la democracia" norteamericana por el ciberespacio, e incluso tiene dudas de si la Internet es una herramienta de liberación o de opresión. Obviamente, la señora Clinton descubrió que la Internet, a pesar de ser un invento yanqui, es como el cuchillo: lo mismo sirve para matar que para cortar el pan, y puede servirle por igual al agresor que al agredido. El uso que se le dé depende de la gente y no de las características de una determinada tecnología.

Es evidente también que sobre sus hombros pesa ahora la experiencia de Wikileaks, un purgante que no ha logrado digerir el gobierno norteamericano, y en particular el Departamento de Estado, obligado a sacar las garras escondidas detrás de la retórica de la libertad de Internet. Con Wikileaks hemos visto todo el arsenal que tienen preparado para los que no quieran asimilarse en torno a los conceptos de la democracia norteamericana: censura, cárcel, cacería financiera, demonización, persecución internacional, apagón cibernético y al final del camino, el "*kill switch"*, el cierre de toda la Internet, que ya fue un sueño del ex presidente George W. Bush.

El gobierno de Obama se propone terminar lo que comenzó su predecesor, aprobar un proyecto de ley que le dé facultades al Presidente de bloquear, sino toda la Internet, por lo menos conexiones en manos del sector privado. La propuesta, que cuenta con el apoyo de los políticos republicanos y demócratas, se debatirá nuevamente este año.

Ya te hablé antes del Ejército Ciberespacial, que entró a operar en plenitud de capacidades el año pasado. Este es simplemente el policía de la Red, mientras que al Departamento de Estado le corresponde blindar la red para que no esté en ella nada que ponga en riesgo la hegemonía norteamericana. La mala noticia es que la lucha por cambiar ese orden de cosas será todavía más dura que lo que hemos visto hasta hoy. La buena, es que jamás se había visto a Estados Unidos tan a la defensiva.

-Cuba ha sido blanco de esa política estadounidense de cara a internet ¿cómo mirar a la Revolución cubana ante la ciberguerra que se le hace?

La circunstancia de la Internet cubana es bastante excepcional. Todos los niños y jóvenes en Cuba han contado con laboratorios de computación desde que comenzaron su vida escolar y hay cientos de miles que han estudiado o estudian carreras informáticas, mientras a los Joven Club de Computación acceden los cubanos de todas las edades. Esta es la inversión más cara que enfrenta hoy cualquier gobierno en cualquier sociedad -la alfabetización digital-, que en la Isla se da por

descontada. Sin embargo, es muy débil la infraestructura de redes y nuestra conexión a la Internet ha sido tardía y con limitaciones de todo tipo, debido al bloqueo de Estados Unidos y a su estrategia de excluir a Cuba de la Internet. Sería divertida, si no fuera tan cínica, la táctica norteamericana de tratar de imponer el reflejo condicionado de que es la Isla la enemiga de Internet, como el ladrón que le grita a su víctima: "¡Ataja!"

Esa alfabetización digital a la que hemos llegado es un elemento esencial para alcanzar una cultura digital, pero no es el único. Cultura es sedimento y, por otra parte, nadie se conecta a la Internet levantando el brazo. Hacen falta tecnologías y velocidad -y por tanto grandes inversiones-, para participar de los recursos y del proceso de innovación permanente que caracteriza la Internet.

A pesar de los pesares y sin que el bloqueo se haya movido un ápice de donde está -son cuentos de camino las famosas "medidas" de Obama para facilitar las telecomunicaciones al pueblo cubano-, Cuba ha dado un paso muy esperanzador para el futuro de la Internet cubana: el cable submarino que nos une con Venezuela. Sabemos que el cable no es la solución mágica a nuestros problemas de conectividad, pero sí que mejorará las comunicaciones y que, al beneficiar a muchos, se cumplirá también en nuestro caso la regla consabida de que los valores en red se fortalecen. Y creo sinceramente que 11 millones de ciberactivistas con los valores de la Revolución cubana generan más pánico en el gobierno de los Estados Unidos que el fantasma de Julian Assange multiplicado.

Anexo 8- Indisciplinas principales asociadas a la Seguridad y Protección de la Información Oficial

- **Asociadas a la telefonía móvil:**
  - Conversaciones que involucren información clasificada o limitada por teléfonos móviles. Peor aun cuando estas conversaciones se tienen en áreas públicas en presencia de otras personas ajenas.
  - Locales de reuniones donde se tratan temas clasificados o limitados y los participantes portan sus teléfonos móviles apagados o no.

- **Asociadas a las computadoras, redes de datos y otros dispositivos modernos:**
  - No determinación ni señalización de cuáles PC están designadas para procesar y almacenar información clasificada y limitada.
  - Procesar información clasificada o Limitada en redes de datos sin la debida protección o a redes globales. Se incluye aquí el caso particular de los dispositivos y redes inalámbricas.
  - Intercambio de información clasificada o Limitada por correo electrónico u otras variantes de mensajería, lo que es negativo cuando se trata de información a emplear en negociaciones en el exterior. Sistemas automatizados para el intercambio obligatorio de informaciones entre organismos y entidades que involucran informaciones clasificadas o Limitadas. Solicitudes de desclasificación de informaciones clasificadas o limitadas para poderlas enviar por medios no protegidos.
  - Descontrol de los dispositivos de almacenamiento removibles.
  - Entrega de información clasificada o Limitada a extranjeros (firmas, consultorías, etc.) sin la debida aprobación.
  - Salidas al exterior del país portando medios o soportes informáticos contentivos de información clasificada o Limitada más allá de la que se requiere para el propósito de la salida y sin aprobación del nivel correspondiente.
  - Deficiente control de la información clasificada o Limitada en medios objeto de reparación o mantenimiento en talleres o por personal no autorizado a conocerla.

Anexo 9- Deficiencias más comunes de la Seguridad Informática en Cuba, según la Oficina de Seguridad para las Redes Informáticas (OSRI)

1. **Deficiente gestión de la seguridad informática.** La gestión de la seguridad informática en la mayoría de las organizaciones es prácticamente nula. La seguridad se ve como un producto y no como un proceso. Se elabora el Plan de Seguridad Informática (PSI) y se implementan controles de seguridad y no se hace más nada hasta que ocurra un incidente.
2. **Delegación de responsabilidades.** El diseño e implementación del Sistema de Seguridad Informática y su gestión se delegan al área de Informática y los directivos se limitan escasamente a aprobarlo. El personal de informática tiene vía libre para casi todas las cosas, desde la introducción o cambio de un equipo hasta la implementación de un nuevo servicio.
3. **Deficiente control y exigencia (o ausencia de ambas cosas).** No se supervisa el trabajo del personal, en particular el de los administradores de redes. No existe un control adecuado de los servicios que brindan las redes de datos, ni la asignación de las cuentas de acceso a estos servicios y su utilización.
4. **Subestimación del factor humano.** No se presta la debida atención a la selección, preparación y concienciación del personal ni al control de sus acciones y las exigencias de sus obligaciones. Se instala un cortafuego y un buen antivirus y se piensa que el problema está resuelto, cuando en realidad la mayoría de los problemas se derivan de la acción del hombre.
5. **Todas las responsabilidades en una misma persona.** Se designa una persona para atender la seguridad sobre la cual caen todas las obligaciones y responsabilidades en esta materia, incluso las que corresponden a otros miembros de la organización.
6. **Sobrevaloración de la tercerización.** Se contrata a una empresa consultora para que lo haga todo, pensando que se tendrá que trabajar menos y que habrá mayor seguridad. La seguridad no es cuestión de una vez, sino de todos los días
7. **Nadie conoce el PSI (solo el que lo elaboró).** Una vez elaborado el plan, se guarda en una gaveta o en la OCIC y se saca solamente cuando se anuncia una inspección.
8. **Se van los inspectores: ya todo terminó.** La seguridad no es vista como una necesidad de la organización y se establece en función de los controles que realizan los niveles superiores. Se trabaja “de control en control”.
9. **Deficiente gestión de contraseñas.** Incumplimiento de las normas establecidas para el empleo de las contraseñas de acceso, al no contar con la estructura y fortaleza requerida, no cambiarse con la debida frecuencia y no garantizarse su privacidad.
10. **Recursos compartidos.** Se comparten archivos, carpetas e incluso discos completos de forma indiscriminada con usuarios que no los requieren para su trabajo y con privilegios de acceso total.
11. **Gestión de trazas de auditoría.** No se analizan las trazas de los eventos para detectar indicios de comportamientos anómalos, limitándose su utilización al momento en que se produce un incidente de seguridad. No se conservan o se conservan solo los de algunos eventos o por un tiempo menor de lo establecido por las normas, debido frecuentemente a mecanismos mal configurados, indiferencia o intencionalidad.

12. **Información de respaldo.** No se realizan copias de seguridad (salvas) de la información crítica de la entidad que permitan la recuperación efectiva después de un incidente. Con frecuencia tampoco se guarda copia de las configuraciones de los sistemas y redes.
13. **Programas malignos.** Deficiente aplicación de los procedimientos establecidos para evitar la introducción y propagación de programas malignos.
14. **Medios removibles.** Empleo indiscriminado de medios removibles (discos externos, dispositivos USB, tarjetas de memoria, CD`s, DVD's), sin autorización ni control.

Anexo 10- Glosario sobre programas malignos y otras amenazas a la Seguridad informática.

Adware- Denominación general dada a los programas patrocinados por algún anunciante y que incluyen publicidad comercial o propaganda política, la cual muestran mientras se emplea el programa. Algunos también recopilan información del usuario y la transmiten a los patrocinadores, en esos casos pudieran considerarse una variante de spyware. En el segundo trimestre de 2010 los adware representaron el 7% de todos los programas malignos detectados.

Ataque distribuido de negación de servicio (DDoS)- Bombardeo simultáneo y abrumador de datos a un mismo servidor o sitio Web, desde múltiples orígenes (generalmente una red zombi), con el fin de hacerlo colapsar e impedir que preste sus servicios.

Backdoor- Programa que abre "puertas traseras" o accesos ocultos a la máquina para permitir traspasar los sistemas de seguridad de la misma y el acceso de hackers a la misma con diferentes fines (control de la máquina, robo o destrucción de información, u otros). Un backdoor puede instalarse mediante un troyano, o por un usuario de la máquina con el fin de permitirle posteriormente el acceso remoto a la misma.

Botnet o red zombi- Red de computadoras bajo control de terceros que las utilizan de forma subrepticia para realizar determinadas funciones de manera autónoma, como pueden ser participar en ataques distribuidos de negación de servicios, envío de spam, o robo de cuentas bancarias. Las botnets pueden tener decenas de miles y hasta millones de computadoras controladas en todo el mundo.

Cookie- Pequeño fichero con información que los servidores de algunas páginas Web hacen copiar al navegador en la computadora del visitante a dicha página, con el fin de recuperar posteriormente esa información cuando el usuario revisite dicha página u otras en las que se hayan colocados códigos ocultos para el control de los visitantes. Aunque las cookies no son programas malignos, debe conocerse que mediante ellas un tercero puede realizar el perfil de un usuario, dando seguimiento a los sitios que visita.

Crimeware- Denominación general dada a los programas que se emplean para cometer acciones delictivas, particularmente contra instituciones financieras.

Data diddler- Programa maligno que efectúa pequeños cambios aleatorios en datos de tablas de cálculo electrónicas o bases de datos volviéndolas inexactas o inútiles.

Exploit- Ataques que aprovechan (explotan) vulnerabilidades conocidas de los sistemas operativos u otros programas. Muchos programas malignos, como por ejemplo los gusanos, utilizan el exploit como vía para poder propagarse. En el segundo trimestre de 2010 representaron el 11% de todos los programas malignos detectados

FraudTool- Variante de programa maligno empleada para realizar estafas (fraudes). Su efectividad radica en su capacidad de convencer al usuario de que realice las acciones que se le piden. Incluye a los pseudoantivirus y a los sitios de phishing, entre otros.

Firmware- Instrucciones de programación para propósitos específicos que vienen grabadas por los fabricantes en memorias de múltiples componentes electrónicos de los equipos para su control

Gusano (Worm)- Programa que es capaz de hacer múltiples réplicas de si mismo y enviarse a otras computadoras a través de la red, generalmente como anexos de correos electrónicos,

mediante archivos compartidos en la red, por sistemas de mensajes instantáneos y en las redes sociales. En el segundo trimestre de 2010 representaron alrededor del 20% de todos los programas malignos detectados. Sus principales variantes son:

Email-worm- Denominación dada a los gusanos que se propagan por la vía del correo electrónico, ya sea por un anexo a un mensaje, o por un hipervínculo en este. Sólo se activan e infectan la máquina si se abre dicho anexo o se accede al hipervínculo.

IM-worm- Denominación dada a los gusanos que se propagan por la vía de los mensajes instantáneos, generalmente enviando un enlace a la lista de contactos del mensaje.

IRC-worm- Denominación dada a los gusanos que se propagan por los canales de chateo, enviando una dirección URL o un fichero infectado que debe ser abierto por el usuario que lo recibe.

Net-worm- Denominación dada a los gusanos que se propagan por la red sin que tenga que intervenir la acción de un usuario, lo que lo hace más peligroso.

P2P-worm- Denominación dada a los gusanos que se propagan a través de las redes de intercambio de ficheros P2P ("peer to peer")

Hoax- Variante digital de las "cartas cadena". Son mensajes con contenido falso que explotan la ingenuidad de los usuarios para que estos hagan copias de los mensajes y los reenvíen a numerosas personas. Los hoax pueden provocar saturación de las redes, además de hacer perder tiempo a los receptores de esos mensajes.

Joke- Programa maligno cuyo fin es embromar o molestar al usuario. Por ejemplo una ventana que cuando se trata de cerrar se mueve o presenta un letrero con un mensaje de burla. La pérdida de tiempo, es el principal daño que ocasionan.

Keylogger- Programa que graba cada golpe de tecla en la máquina durante un período de tiempo con el fin de recuperar posteriormente dicha información contentiva de información confidencial, como nombres de usuario, claves y otras. Un keylogger puede ser instalado de forma remota y enviar por correo la información de forma oculta, pero también puede ser instalado por un usuario de la máquina quien luego recogerá el informe suministrado por el programa.

Password stealer o PWS- Programas empleados para obtener los password (claves) de una computadora. Puede ser instalado directamente por un usuario para conocer las claves de otros usuarios, o introducirse como un troyano del tipo Trojan-PSW.

Phishing- Variante de estafa informática por la que, empleando técnicas de ingeniería social, se solicita a los usuarios información confidencial como números de cuentas bancarias o de tarjetas de créditos, claves de acceso u otras informaciones, para lo cual se le presentan al usuario direcciones de correo y hasta páginas Web idénticas a las reales pero que redireccionan hacia el estafador la información introducida en ellas.

Pornware- Denominación dada a los programas que, como troyano o instalados deliberadamente por los usuarios, brindan facilidades para la obtención de material pornográfico, ya sea descargándolo directamente de la red a la computadora (porn-downloader), marcando servicios sexuales telefónicos (porn-dialer) o haciendo búsquedas de sitios porno en Internet (porn-tool)

Ransomware- Programa maligno que encripta la información de la máquina y pide el pago de un rescate (ransom) a cambio de la clave para desencriptarlos.

Riskware- Denominación general a dada a los programas comerciales legales, diseñados para propósitos lícitos, pero que pueden utilizarse también para cometer acciones ilegales o perniciosas, como pueden ser las utilidades para administración remota de equipos, para manejo de claves o para monitoreo de la actividad de las computadoras, entre otros.

Rogue Security Software o Pseudoantivirus- Variante de programa maligno que muestran mensajes sobre la detección de programas nocivos, convencen al usuario de la existencia de amenazas para el ordenador (que en realidad no existen), en ocasiones provocando ellos mismos los fallos, y lo estimulan a descargar un antivirus libre de pago que una vez descargado comienza un supuesto escaneo y detección de infecciones en la máquina, para finalmente ofrecer corregir los errores supuestamente detectados y desinfectar el sistema, a cambio de un módico pago.

Rootkit- Denominación dada tanto a los procedimientos de ocultación de ficheros y carpetas como a los programas que se utilizan para ello. El procedimiento de rootkit es ampliamente empleado por los programas malignos para ocultar su presencia, pero también puede ser utilizado por los usuarios para ocultar en sus máquinas información comprometedora o no autorizada mediante programas comerciales sencillos elaborados con este fin.

Spam o correo basura- Mensajes de correo electrónico no solicitado, generalmente provenientes de una dirección de correo falsa. Pueden ser de tipo publicitario, aunque muchas veces son una vía de realizar ataques de negación de servicios consumiendo el ancho de banda. El spam se ha extendido a otras áreas como los foros de discusión en Internet y también a la telefonía celular.

SpamTool- Programa que envía grandes cantidades de spam. Puede pertenecer a un usuario que voluntariamente lo instala con ese fin, o instalarse como un troyano que realiza esa función, denominado entonces Trojan-spammer.

Spoof- Variedad de ataque en la que una página Web o un correo electrónico es falsificado para que parezca provenir de una fuente verdadera de confianza. El spoof se emplea a menudo como vía para diseminar programas malignos.

SpooferTool- Programa diseñado para crear spoof.

Spyware- Denominación general dada a los programas que recolectan información y la envían a un destinatario dado de forma oculta. Algunos spyware tienen el objetivo de recopilar los hábitos de los usuarios, como sus sitios más visitados, programas más utilizados o incluso la forma en que utilizan un juego determinado, con fines de trazar estrategias comerciales o de diseño de productos, pero otros se destinan para obtener datos confidenciales con fines más peligrosos. Los keyloggers y la mayoría de los troyanos entran en esta clase.

Troyano (trojan)- Programa maligno que penetra a la máquina subrepticiamente utilizando múltiples vías de infectación, y está programado para cumplir una o varias funciones en la misma de forma oculta. Existen variadas clases de troyanos, atendiendo a dichas funciones.

Trojan-ArcBomb- Variante de troyano diseñada para ralentizar o hacer colapsar el funcionamiento de la computadora mediante la generación de gran cantidad de datos o ficheros repetidos, en blanco o corruptos.

Trojan-Banker- Variante de troyano diseñada para robar los datos del usuario relativos a sistemas bancarios on-line o de tarjetas de crédito.

Trojan-Clicker- Variedad de troyano que obliga al sistema a visitar una página Web específica. Puede tener como objetivo obligar al usuario a visitar el sitio con fines de

promoción comercial o política; o también con el fin de hacer colapsar el sitio visitado como parte de un ataque de negación de servicio. En el segundo trimestre de 2010 representaban casi el 7% de todos los programas malignos detectados

Trojan-DDoS- Variedad de troyano diseñado para hacer ataques de negación de servicios.

Trojan-Downloader- Variedad de troyano de muy pequeño tamaño que descarga de otro sitios y ejecuta subrepticiamente otros programas más complejos como pueden ser otros troyanos, adware o spyware. En el segundo trimestre de 2010 representaron el 15% de todos los programas malignos detectados.

Trojan-Dropper- Variante de troyano poco común, cuya función es instalar un virus en la computadora. Al portar dentro de si el código del virus, el troyano impide que sea reconocido por los antivirus que normalmente lo detectarían, antes de que sea instalado en la máquina.

Trojan-IM- Variante de troyano diseñada para robar los datos del usuario (nombre de usuario, claves) relativos a programas de mensajería instantánea como MSN Messenger, Skype y otros.

Trojan-Mailfinder- Variante de troyano diseñada para recopilar y robar las direcciones de correo electrónico almacenadas en la computadora.

Trojan-Notifier- Variante de troyano diseñada para informar al hacker que la computadora infectada se encuentra activa y conectada a la red, así como los datos del equipo (dirección IP, puertos abiertos, etc)

Trojan-Proxy- Variante de troyano diseñada para dar acceso a Internet al hacker, a través de la computadora infectada, utilizando las facilidades de conexión de su usuario.

Trojan-PSW- Variante de troyano diseñada para robar los password (claves) de los usuarios de una computadora.

Trojan-Ransom- Variante de troyano diseñada para "secuestrar" la información de la máquina, encriptando la información hasta que se pague un rescate a cambio de la clave para desencriptarlos

Trojan-SMS- Variante de troyano diseñada para enviar mensajes de texto (SMS) desde teléfonos móviles infectados.

Trojan-Spy- Variante de troyano diseñada para espiar las acciones que ejecuta el usuario de una computadora, como puede ser lo que marca en el teclado o lo que está viendo en la pantalla y enviárselo a alguien.

Virus- Programa maligno que se replica, adjuntándose o insertándose en el código de otros programas, produciendo mal funcionamiento de estos, destrucción de información o incluso la interrupción del funcionamiento de la máquina.

Virus macro- Tipo de virus que explota los lenguajes de automatización de tareas (conocidos como "macros") de algunos programas, especialmente los del paquete ofimático MSOffice. Fueron especialmente peligrosos en la década de los 90, pero desde la aparición del MSOffice 2000 y sus posteriores versiones, su prevalencia se redujo notablemente.

Bombas lógicas- Variedad de virus que sólo se activa ante la ocurrencia de determinadas condiciones: una fecha dada, ejecutar una combinación de teclas determinada, u otras.

UM-2500

R-5991

Feccha