Universidad de Ciencias Pedagógicas
"Rafael María de Mendive". Pinar del Río, Cuba.
Año 10/No.39/abr-jun/2012/RNPS 2057/ISSN 1815-7696
Recibido:16/01/2012 Aprobado: 20/03/2012

La seguridad informática es un componente esencial de la Seguridad Nacional

Informatics Security as an essential component of National Security

Autores: MSc. Alina Alfonso Morejón; Lic. Hugo César Arocha Domínguez

Email: alinam@ucp.pr.rimed.cu; hugo@ucp.pr.rimed.cu

Centro de procedencia: Universidad de Ciencias Pedagógicas "Rafael María de Mendive"

Resumen:
La revolución científico técnica y la informatización social en su desarrollo vertiginoso, demuestran cada vez más la necesidad de elevar la cultura informática en aras de aprovechar las bondades de la mediación tecnológica en los procesos sociales, sin embargo, el aprovechamiento de estos medios implica riesgos de alcance: personal, institucional, nacional y extraterritorial, por lo que la seguridad informática ha devenido en componente de la Seguridad Nacional, en tanto puede constituir un arma poderosa para penetrar y atacar objetivos estatales, económicos y militares de significativa importancia para el país.

Palabras claves: Seguridad informática, seguridad nacional.

Abstract:
The scientific-technical revolution and the social informativeness in their vertiginous development constantly show the necessity to upgrade the culture in Informatics so as to take advantages of the possibilities given by technology in favour of the social processes. However, using these media imply having risks at different levels: personal, institutional, national, and even extraterritorial. That is why, computer security has become one of the components of National Security because it can be a powerful weapon to penetrate and attack objectives of the state in the fields of economy and the army, which is of great importance for the country.

Keywords: Informatics Security, National Security

La seguridad nacional, una necesaria condición del estado.

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; 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".*[1]

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".*[2]

---

[1] *Castro Ruz Fidel. Discurso pronunciado en Santiago de Cuba, en ocasión del 45 Aniversario del Asalto al Cuartel Moncada, julio 26 de 1998.*
[2] *Martí Pérez José. "El Partido Revolucionario Cubano". Patria, 3 de marzo de 1892.*

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 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.

La siguiente frase expresada por el Comandante en Jefe en alusión a Martí, sintetiza la esencia del **concepto de Seguridad Nacionalde 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".*[3]

La seguridad informática como parte de la 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.

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**.

Se asume 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.

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*

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

será por encima de todo más rico cuanto más cultura política tenga, cuanto más preparación tenga, ***cuanto más información tenga****…"*[4]*.*

Por estas razones, la Seguridad de la Información es una de las dimensiones de la Seguridad Nacional de Cuba.

La **Seguridad de la Información**se define como: *la condición necesaria alcanzada por cada institución para garantizar la disponibilidad, confidencialidad e integridad de la información que este necesita emplear para su desarrollo y defensa.*
Estos requisitos de todo sistema de información consisten en:

- Buscar, obtener, diseminar y organizar la información, de forma tal que todo usuario autorizado que la necesite, pueda acceder a ella oportunamente (esto se conoce como **Disponibilidad**).
- Impedir el acceso a la información disponible a aquel que no tenga autorización para utilizarla. (esto se conoce como **Confidencialidad**).
- Evita la alteración o destrucción no autorizada de la información disponible (esto se conoce como **Integridad**).

Por lo que el concepto de **Protección a la información**se refiere precisamente al *conjunto de acciones dirigidas a asegurar la integridad, la confidencialidad y la disponibilidad de la información con que cuenta el país y cada una de sus instituciones*. Por tanto, esta constituye además una rama o esfera de la Seguridad de la Información.

Se entiende 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.

Las amenazas relacionadas conla 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 obstáculo a la divulgación y conocimiento en el exterior de los logros del socialismo en nuestro país, o la ayuda solidaria a otros pueblos.

En el interior del país también 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 conla posibilidad de destrucción o alteración de información, abarcan un universo amplio de acciones u omisiones provenientes del enemigo externo, elementos

[4] *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*

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 las que tienen conocimiento exclusivo.
- 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.

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 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 losEUA 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**, 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 puedan incrementarse en número, variedad y alcance en el futuro.

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 el consensopara alcanzar los intereses y objetivos nacionales y en la capacidad y voluntad de resistencia para desarrollarse, defenderse y vencer en las más difíciles circunstancias. Como principio, la política nacional en relación con la Seguridad de la Información, se basa en acciones que garanticen la preservación de nuestros intereses y objetivos nacionales, sin detrimento 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.

BIBLIOGRAFÍA.

1. Manunta, G. Seguridad una Introducción.Revista Seguridad Corporativa. http://www.seguridadcorporativa.org
2. Álvarez Marañón, Gonzalo; Pérez García, Pedro Pablo. Seguridad informática para empresas y particulares. Editorial McGraw – Hill. 2004.
3. Stallings, William. Fundamentos de seguridad en redes. aplicaciones y estándares. Prentice-Hall Inc.2003.
4. Morant Ramón, J.L.; Ribagorda Garnacho, A.; Sancho Rodríguez J. Seguridad y protección de la información. Colección de Informática, Editorial Centro de Estudios Ramón Areces, S.A., Madrid. 1994.
5. Resoluciones 6/96 del Ministerio del Interior. Reglamento sobre la Seguridad Informática
6. Resolución .188/2006 del Ministerio del Trabajo y Seguridad Social sobre los Reglamentos Disciplinarios Internos del 21 de agosto de 2006.
7. Resolución 127/07 Ministerio de la Informática y las Comunicaciones. Reglamento de Seguridad para las Tecnologías de la Información.
8. Resolución 176/07 MINED Reglamento de Seguridad Informática en la Actividad Educacional del Ministerio de Educación.