**XXXI TALLER CIENTÍFICO DE EDUCACIÓN PATRIÓTICO MILITAR E INTERNACIONALISTA CON LOS CENTROS DE EDUCACIÓN SUPERIOR DE LA REGIÓN OCCIDENTAL**

**PONENCIA**

**LA SEGURIDAD INFORMÁTICA COMO DIMENSIÓN DE LA SEGURIDAD NACIONAL DE CUBA. SU IMPRTANCIA EN LAS CONDICIONES ACTUALES**

**Autores:**

**Herbert Ibarra Betancourt**

**Yanelys García García**

**1er. año de Geografía**

**Tutor: Cor. ® Dr. C. Jesús Martínez Pedroso**

**Profesor Titular**

**UCPEJV**

**RESUMEN**

El presente trabajo tiene como finalidad esencial abordar la concepción que tiene los autores acerca de la seguridad informática en las condiciones actuales, cuando se está desarrollando la 4ta. revolución tecnológica. Los autores tienen en cuenta que 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. Como efecto de la revolución que se está produciendo en el campo de las Tecnologías de la Información y las Comunicaciones, a pesar de los raudos avances, trae consigo también nuevos riesgos y amenazas que pueden poner en peligro la seguridad nacional de cualquier país. Surge entonces la necesidad de garantizar la seguridad informática. Los autores son de la consideración de que Cuba, pese al bloqueo tecnológico a la que la tiene sometida el imperialismo yanqui elimina cada vez más las brechas en ese sentido y logra desarrollar su propia estrategia de seguridad informática, convirtiéndose en referente mundial en ese campo.

**Palabras clave: seguridad, informática, revolución, tecnologías, información, comunicaciones.**

**Introducción**

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.

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.

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.

Como efecto de la revolución que se está produciendo en el campo de las Tecnologías de la Información, si bien ello significa una gran paso de avance y un salto de calidad indiscutible, surgen también nuevos riesgos, amenazas y agresiones que pueden poner en peligro la seguridad nacional de cualquier país. Surge entonces la necesidad de garantizar la seguridad informática.

El presente trabajo es el resultado de una investigación que realiza el autor sobre ese importante tema y tiene como objetivo fundamental proporcionar algunas ideas acerca de cómo se puede garantizar la Seguridad Informática en las instituciones estatales, sociales, económicas, educacionales y otras, lo que debe formas parte de una cultura informática en ese sentido.

1. **Fundamentos teóricos y generalidades**

La seguridad informática o seguridad de tecnologías de la información es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software (bases de datos, metadatos, archivos), hardware y todo lo que la organización valore (activo) y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada.

El concepto de seguridad de la información no debe ser confundido con el de «seguridad informática», ya que este último solo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos.

La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.

La seguridad informática debe establecer normas que minimicen los riesgos a la información o infraestructura informática. Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática minimizando el impacto en el desempeño de los trabajadores y de la organización en general y como principal contribuyente al uso de programas realizados por programadores.

La seguridad informática está concebida para proteger los activos informáticos, entre los que se encuentran los siguientes:

**La infraestructura computacional:** Es una parte fundamental para el almacenamiento y gestión de la información, así como para el funcionamiento mismo de la organización. La función de la seguridad informática en esta área es velar que los equipos funcionen adecuadamente y anticiparse en caso de fallas, robos, incendios, boicot, desastres naturales, fallas en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática.

**Los usuarios**: Son las personas que utilizan la estructura tecnológica, zona de comunicaciones y que gestionan la información. Debe protegerse el sistema en general para que el uso por parte de ellos no pueda poner en entredicho la seguridad de la información y tampoco que la información que manejan o almacenan sea vulnerable.

**La información**: es el principal activo. Utiliza y reside en la infraestructura computacional y es utilizada por los usuarios.

1. **Riesgos, amenazas y agresiones en el campo de la Seguridad Informática y sus impactos en la Seguridad Nacional de Cuba.**

No solo las amenazas que surgen de la programación y el funcionamiento de un dispositivo de almacenamiento, transmisión o proceso deben ser consideradas, también hay otras circunstancias que deben ser tenidas en cuenta, incluso «no informáticas». Muchas son a menudo imprevisibles o inevitables, de modo que las únicas protecciones posibles son las redundancias y la descentralización, por ejemplo mediante determinadas estructuras de redes en el caso de las comunicaciones o servidores en clúster para la disponibilidad.

Las amenazas pueden ser causadas por:

* **Usuarios**: causa del mayor problema ligado a la seguridad de un sistema informático. En algunos casos sus acciones causan problemas de seguridad, si bien en la mayoría de los casos es porque tienen permisos sobre dimensionados, no se les han restringido acciones innecesarias, etc.
* **Programas maliciosos**: programas destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema. Es instalado (por inatención o maldad) en el ordenador, abriendo una puerta a intrusos o bien modificando los datos. Estos programas pueden ser un virus informático, un gusano informático, un troyano, una bomba lógica, un programa espía o spyware, en general conocidos como malware.
* **Errores de programación**: La mayoría de los errores de programación que se pueden considerar como una amenaza informática es por su condición de poder ser usados como exploits por los crackers, aunque se dan casos donde el mal desarrollo es, en sí mismo, una amenaza. La actualización de parches de los sistemas operativos y aplicaciones permite evitar este tipo de amenazas.
* I**ntrusos**: persona que consiguen acceder a los datos o programas a los cuales no están autorizados (crackers, defacers, hackers, script kiddie o script boy, viruxers, etc.).
* **Un siniestro (robo, incendio, inundación):** una mala manipulación o una mala intención derivan a la pérdida del material o de los archivos.
* **Personal técnico interno**: técnicos de sistemas, administradores de bases de datos, técnicos de desarrollo, etc. Los motivos que se encuentran entre los habituales son: disputas internas, problemas laborales, despidos, fines lucrativos, espionaje, etc.
* **Fallos electrónicos o lógicos** de los sistemas informáticos en general.
* **Catástrofes naturales**: rayos, terremotos, inundaciones, rayos cósmicos, etc.
* **Vulnerabilidad del usuario.**

**Tipos de amenaza**

**Amenazas por el origen**

El hecho de conectar una red a un entorno externo da la posibilidad de que algún atacante pueda entrar en ella, con esto, se puede hacer robo de información o alterar el funcionamiento de la red. Sin embargo el hecho de que la red no esté conectada a un entorno externo, como Internet, no garantiza la seguridad de la misma. De acuerdo con el Computer Security Institute (CSI) de San Francisco aproximadamente entre el 60 y 80 por ciento de los incidentes de red son causados desde dentro de la misma. Basado en el origen del ataque podemos decir que existen dos tipos de amenazas:

1. **Amenazas internas**: Generalmente estas amenazas pueden ser más serias que las externas por varias razones como son: Si es por usuarios o personal técnico, conocen la red y saben cómo es su funcionamiento, ubicación de la información, datos de interés, etc. Además tienen algún nivel de acceso a la red por las mismas necesidades de su trabajo, lo que les permite unos mínimos de movimientos. Los sistemas de prevención de intrusos o IPS, y firewalls son mecanismos no efectivos en amenazas internas por, habitualmente, no estar orientados al tráfico interno. Que el ataque sea interno no tiene que ser exclusivamente por personas ajenas a la red, podría ser por vulnerabilidades que permiten acceder a la red directamente: rosetas accesibles, redes inalámbricas desprotegidas, equipos sin vigilancia, etc.
2. **Amenazas externas**: Son aquellas amenazas que se originan fuera de la red. Al no tener información certera de la red, un atacante tiene que realizar ciertos pasos para poder conocer qué es lo que hay en ella y buscar la manera de atacarla. La ventaja que se tiene en este caso es que el administrador de la red puede prevenir una buena parte de los ataques externos.

**Amenazas por el efecto**

El tipo de amenazas por el efecto que causan a quien recibe los ataques podría clasificarse en:

* Robo de información.
* Destrucción de información.
* Anulación del funcionamiento de los sistemas o efectos que tiendan a ello.
* Suplantación de la identidad, publicidad de datos personales o confidenciales, cambio de información, venta de datos personales, etc.
* Robo de dinero, estafas y otras.

**Amenazas por el medio utilizado**

Se pueden clasificar por el modus operandi del atacante, si bien el efecto puede ser distinto para un mismo tipo de ataque:

* **Virus informático:** malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en un computadora, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos.
* **Phishing.**
* **Ingeniería social.**
* **Denegación de servicio.**

**Amenaza informática del futuro**

Si en un momento el objetivo de los ataques fue cambiar las plataformas tecnológicas ahora las tendencias cibercriminales indican que la nueva modalidad es manipular los certificados que contienen la información digital. El área semántica, era reservada para los humanos, se convirtió ahora en el núcleo de los ataques debido a la evolución de la Web 2.0 y las redes sociales, factores que llevaron al nacimiento de la generación 3.0.

Se puede afirmar que “la Web 3.0 otorga contenidos y significados de manera tal que pueden ser comprendidos por las computadoras, las cuales -por medio de técnicas de inteligencia artificial- son capaces de emular y mejorar la obtención de conocimiento, hasta el momento reservada a las personas”.

Es decir, se trata de dotar de significado a las páginas Web, y de ahí el nombre de Web semántica o Sociedad del Conocimiento, como evolución de la ya pasada Sociedad de la Información

En este sentido, las amenazas informáticas que viene en el futuro ya no son con la inclusión de troyanos en los sistemas o softwares espías, sino con el hecho de que los ataques se han profesionalizado y manipulan el significado del contenido virtual.

Obtención de perfiles de los usuarios por medios, en un principio, lícitos: seguimiento de las búsquedas realizadas, históricos de navegación, seguimiento con geo posicionamiento de los móviles, análisis de las imágenes digitales subidas a Internet, etc.

**Análisis de riesgos informáticos**

Ante la situación planteada y a los efectos de garantizar la Seguridad Informática se impone la necesidad de efectuar el **análisis de riesgos informáticos.** Este análisis es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

Teniendo en cuenta que la explotación de un riesgo causaría daños o pérdidas financieras o administrativas a una empresa u organización, se tiene la necesidad de poder estimar la magnitud del impacto del riesgo a que se encuentra expuesta mediante la aplicación de controles. Dichos controles, para que sean efectivos, deben ser implementados en conjunto formando una arquitectura de seguridad con la finalidad de preservar las propiedades de confidencialidad, integridad y disponibilidad de los recursos objetos de riesgo.

Es importante tener en cuenta que el activo más importante que se posee es la información y, por lo tanto, deben existir técnicas que la aseguren, más allá de la seguridad física que se establezca sobre los equipos en los cuales se almacena. Estas técnicas las brinda la seguridad lógica que consiste en la aplicación de barreras y procedimientos que resguardan el acceso a los datos y solo permiten acceder a ellos a las personas autorizadas para hacerlo.

Cada tipo de ataque y cada sistema requiere de un medio de protección o más (en la mayoría de los casos es una combinación de varios de ellos). A los efectos de garantizar la seguridad nacional se deben tener en cuenta las medidas que se consideran básicas para asegurar un sistema tipo, si bien para necesidades específicas se requieren medidas extraordinarias y de mayor profundidad:

* Utilizar técnicas de desarrollo que cumplan con los criterios de seguridad al uso para todo el software que se implante en los sistemas, partiendo de estándares y de personal suficientemente formado y concienciado con la seguridad.
* Implantar medidas de seguridad físicas: sistemas anti incendios, vigilancia de los centros de proceso de datos, sistemas de protección contra inundaciones, protecciones eléctricas contra apagones y sobretensiones, sistemas de control de accesos, etc.
* Establecer contraseñas difíciles de averiguar que, por ejemplo, no puedan ser deducidas a partir de los datos personales del individuo o por comparación con un diccionario, y que se cambien con la suficiente periodicidad. Las contraseñas, además, deben tener la suficiente complejidad como para que un atacante no pueda deducirla por medio de programas informáticos. El uso de certificados digitales mejora la seguridad frente al simple uso de contraseñas.
* Utilizar tecnologías repelentes o protectoras: cortafuegos, sistema de detección de intrusos - antispyware, antivirus, llaves para protección de software, etc. Mantener los sistemas de información con las actualizaciones que más impacten en la seguridad.
* Utilizar copias de seguridad e, incluso, sistemas de respaldo remoto que permiten mantener la información en dos ubicaciones de forma asíncrona.
* Restringir el acceso (de personas de la organización y de las que no lo son) a los programas y archivos.
* Asegurar que la información transmitida sea la misma que reciba el destinatario al cual se ha enviado y que no le llegue a otro. y que existan sistemas y pasos de emergencia alternativos de transmisión entre diferentes puntos.
* Organizar a cada uno de los empleados por jerarquía informática, con claves distintas y permisos bien establecidos, en todos y cada uno de los sistemas o aplicaciones empleadas.
* Actualizar constantemente las contraseñas de accesos a los sistemas de cómputo, como se ha indicado más arriba, e incluso utilizando programa que ayuden a los usuarios a la gestión de la gran cantidad de contraseñas que tienen gestionar en los entornos actuales, conocidos habitualmente como gestores de identidad.

En general los programas antivirus no son capaces de detectar todas las posibles formas de contagio existentes, ni las nuevas que pudieran aparecer conforme los ordenadores aumenten las capacidades de comunicación, además los antivirus son vulnerables a desbordamientos de búfer que hacen que la seguridad del sistema operativo se vea más afectada aún, aunque se considera como una de las medidas preventivas indispensable.

Existen diferentes tipos de ataques en Internet como virus, troyanos u otros, dichos ataques pueden ser contrarrestados o eliminados pero hay un tipo de ataque, que no afecta directamente a los ordenadores, sino a sus usuarios, conocidos como “el eslabón más débil”. Dicho ataque es capaz de conseguir resultados similares a un ataque a través de la red, saltándose toda la infraestructura creada para combatir programas maliciosos. Además, es un ataque más eficiente, debido a que es más complejo de calcular y prever. Se pueden utilizar infinidad de influencias psicológicas para lograr que los ataques a un servidor sean lo más sencillo posible, ya que el usuario estaría inconscientemente dando autorización para que dicha inducción se vea finiquitada hasta el punto de accesos de administrador.

Existen, además, infinidad de modos de clasificar un ataque y cada ataque puede recibir más de una clasificación. Por ejemplo, un caso de phishing puede llegar a robar la contraseña de un usuario de una red social y con ella realizar una suplantación de la identidad para un posterior acoso, o el robo de la contraseña puede usarse simplemente para cambiar la foto del perfil y dejarlo todo en una broma (sin que deje de ser delito en ambos casos, al menos en países con legislación para el caso, como lo es España).

**Conclusiones**

El concepto de seguridad de la información no debe ser confundido con el de «seguridad informática», ya que este último solo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos.

La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.

La seguridad informática está concebida para proteger los activos informáticos, entre los que se encuentran los siguientes: La infraestructura computacional, los usuarios y la información.

No solo las amenazas que surgen de la programación y el funcionamiento de un dispositivo de almacenamiento, transmisión o proceso deben ser consideradas, también hay otras circunstancias que deben ser tenidas en cuenta, incluso «no informáticas», muchas de las cuales suelen ser a menudo imprevisibles o inevitables, de modo que las únicas protecciones posibles son las redundancias y la descentralización. Estas amenazas pueden tener diferentes causas, lo más importante es identificarlas y tenerlas en cuenta.

La Seguridad Informática debe ser estudiada como ciencia para que no impida el trabajo de los operadores en lo que les es necesario y que puedan utilizar el sistema informático con toda confianza, de ahí la necesidad de elaborar la correspondiente política de seguridad.

Por cuanto cada tipo de ataque y cada sistema requiere de un medio de protección o más (en la mayoría de los casos es una combinación de varios de ellos), a los efectos de garantizar la seguridad nacional se deben tener en cuenta las medidas que se consideran básicas para asegurar un sistema tipo, si bien para necesidades específicas se requieren medidas extraordinarias y de mayor profundidad.

Para los maestros en formación resulta de vital importancia la adquisición de los conocimientos acerca de la Seguridad Informática para así educar a sus alumnos en las medidas que la garanticen frente a los riesgos, amenazas y agresiones que se derivan principalmente de la actividad enemiga.

**Bibliografía**

1. Colegio de Defensa Nacional y DIEM-MES. Material de Estudio. La Habana, 2008
2. Colegio de Defensa Nacional. Fundamentos de la Seguridad Nacional. La Habana, 2008
3. La Seguridad Nacional ante los retos de las nuevas tecnologías de la información. Compilación del CODEN. 2011
4. Castro Ruz, Fidel. “La sublevación en la ONU”. Reflexiones del compañero Fidel. Periódico Granma Digital. www.granma.co.cu . Consultado 10/11/2010
5. Decreto – Ley 35 de las telecomunicaciones, las tecnologías de la información y la comunicación y el uso del espectro radioeléctrico. 2021.
6. Material de estudio del PCC La Informatización de la sociedad cubana. Situación actual y perspectivas. 2015
7. Pérez Salomón, Omar. Guerra Cibernética made in USA. Boletín Cubarte 2010.