## ARTICULO DE POSICIÓN

**Título: La informática y la seguridad. Un tema de importancia para el directivo.**

**Title: Informatics and security: an important topic for managers.**

**Autores:** Gonzalo García Pierrat, [I] María Josefina Vidal Ledo. [II]

I. Licenciado en Ciencias de la Computación. Oficina de Seguridad para las Redes Informáticas

II. Licenciada en Cibernética Matemática. Profesora Consultante e Investigador Auxiliar. Escuela Nacional de Salud Pública.

**RESUMEN**:

**Introducción**: El proceso de transformación de la sociedad que se manifiesta en todos los sentidos, tiene como base la tecnología. Sin embargo, ¿Ofrece seguridad el uso de las tecnologías de la información?

**Objetivo:** Fomentar una cultura informática en aquellos que trazan políticas y utilizan las tecnologías en los procesos organizacionales.

**Métodos**: El examen de los argumentos ha sido fruto de revisiones, experiencias e intercambios.

**Resultados**: Se argumenta en la importancia de la seguridad informática, en sus tres aspectos: la *confidencialidad*, la *integridad* y la *disponibilidad**;*** tanto para directivos, a quienes corresponde la máxima responsabilidad de organizar la política y estrategia de uso y preservación de todos estos procesos informativos y tecnológicos tan requeridos en la toma de decisiones de la esfera que dirigen; funcionarios que operan tanto las tecnologías como la información en ellas contenidas, especialistas de informática a los que corresponde garantizar el soporte seguro donde operan estas técnicas; el personal encargado de la seguridad y protección que garantiza el cumplimiento de las políticas, medidas y contramedidas empleadas para asegurar los medios, repositorios e información misma. Los aspectos fundamentales para identificar y gestionar las amenazas, riesgos y vulnerabilidades a los que está sometido el sistema informático y la implementación de controles para minimizarlos.

**Conclusión:** El trabajo hace énfasis en los principios fundamentales de la seguridad informática, el análisis y gestión de riesgos, las políticas, medidas, contramedidas y procedimientos que garanticen la seguridad del sistema de información de las instituciones en el actual proceso de informatización de la sociedad

**Palabras Clave**: Tecnologías informáticas, Informatización, seguridad informática,

**ABSTRACT**:

**Introduction:** The societal transformation process understood in many senses is based on technology. Nevertheless, does the use of information technology offer security?

**Objective:** To promote an information culture in individuals who outline policies and use technologies in organizational processes.

**Methods**: Arguments examination is the result of reviews, experiences and exchanges.
Results: Informatics is based on the importance of the information security in 3 aspects: confidentiality, integrality and availability which are important to leadership responsible for organizing policy and strategies for using and preserving all these information processes and technological so much-needed in decision-making in the field they run; to officials handling technologies as well as information contained in it; to specialists in informatics responsible for assuring a safe support where these techniques operate; to the staff in charge of security and protection assuring the implementation of policies, measures and countermeasures applied to assure the means, repositories and information itself.
**Conclusion**: The document emphasizes the main principles of information security, analysis and risk management, policies, measures and countermeasures and other procedures assuring the safety of the information system at institutions in the existing information process at the society.

**Key words**: Informatics technology, computerization, informatics security.

## INTRODUCCIÓN

En la actualidad se puede apreciar un proceso de transformación de la sociedad que se manifiesta en todos los sentidos, provocado por la incesante aparición de modernas tecnologías, portadoras de soluciones, aplicaciones y servicios de todo tipo que modifican radicalmente las formas de hacer y de vivir que se han moldeado a través de muchas generaciones. [1,2]

El mundo cambia constantemente y al igual que el ser humano, unos lo hacen de manera natural y se adaptan a gran velocidad a los nuevos tiempos, mientras que otros confrontan lo desconocido conservadoramente, con reserva, lentitud y cierto temor a lo que pueda suceder o en el peor de los casos – por suerte cada vez menos - se niegan rotundamente a participar en esta nueva aventura de la humanidad. [3]

Las actuales generaciones, nacidas bajo el influjo de las nuevas tecnologías caen de manera natural en el primer grupo y sus integrantes han sido denominados, por los que gustan de clasificarlo todo, como "nativos digitales", mientras que aquellos que nacieron en épocas anteriores, donde predominaban los artefactos analógicos, pasan más trabajo para asimilar la nueva ciencia y suelen ser referidos, en los casos más extremos, como "inmigrantes digitales".[4, 5]

Hoy se vive en un mundo que se encuentra en sostenido proceso de informatización. Nuevos dispositivos de diversos tipos cada vez más pequeños aparecen por doquier, integran funciones diversas, consumen muy poca energía y son portables e inalámbricos.

Los niños de hoy juegan con esas tecnologías con mayor facilidad y destreza con la que sus padres solían patinar o montar bicicleta, oyen más música en un día que la que ellos oían en semanas y explican el funcionamiento de los equipos que salen al mercado sin necesidad de leer las instrucciones que los acompañan. Les ha tocado nacer y desarrollarse simultáneamente con el surgimiento y evolución de las nuevas tecnologías de informática y comunicaciones y por ello las comprenden con la misma naturalidad con que asimilan las palabras del lenguaje que les sirven para comunicarse.

Muchas personas mayores sin embargo, se resisten a incorporar estas tecnologías a sus actividades habituales, bajo el falso pretexto de que no las necesitan, que sin ellas logran lo que se proponen en su campo de acción y que su empleo les resulta

muy complicado. Pero en el fondo esos son solo pretextos y la verdadera razón generalmente es el miedo, pues temen no solo que algo salga mal, sino demostrar ineptitud en faenas en las que siempre han cosechado éxitos. [4, 5]

Como en otros ámbitos, aquí también aparece la resistencia al cambio, la oposición a lo diferente y ante cada nuevo adelanto tecnológico no faltan los enemigos y detractores, para lo que con frecuencia emplean como argumento la aparición de mayores riesgos. [3]

Cuando los primeros automóviles comenzaron a rodar por campos y ciudades, no alcanzaban velocidades mayores de 30 kilómetros por hora, no obstante sus críticos los consideraban un gran peligro para la población, injuriaban a sus osados conductores e insistían con denuedo en la continuidad del empleo de los vehículos de tracción animal. Lo mismo podría decirse de los distintos tipos de embarcaciones marítimas, naves aéreas, calderas de vapor, energía nuclear, por solo citar algunos ejemplos de revolucionarias innovaciones a través de la historia.

Cada uno de estos desarrollos fue el resultado de un largo proceso de perfeccionamiento que transitó desde su concepción inicial hasta lograr la posibilidad de su utilización eficaz y con una relativa seguridad.[6]

Ahora bien, ¿Ofrecen seguridad las tecnologías de la información? ¿Cómo se pueden utilizar de manera segura? ¿Existen riesgos en su empleo?

El propósito de este trabajo es fomentar una cultura informática en aquellos, sean nativos o inmigrantes, que trazan políticas y utilizan las tecnologías en los procesos organizacionales.

El examen de los argumentos aquí expuestos, fruto de revisiones, experiencias e intercambios, sin dudas, ha de contribuir de alguna manera a conocer más sobre las tecnologías de la informática y las comunicaciones, sus aplicaciones y servicios y fundamentalmente a la generalización de las buenas prácticas que conduzcan a su empleo eficiente y seguro.[7]

## DESARROLLO

### Importancia de la Seguridad Informática. [8]

Numerosas anécdotas ilustran la importancia de la seguridad informática:

- "Un amigo contaba las dificultades confrontadas durante una gestión de compra en la oficina comercial de una empresa suministradora, pues resulta que en varias ocasiones, a pesar de la necesidad que tenía y la persistencia mostrada, no pudo realizar la operación debido a que el sistema automatizado se encontraba fuera de servicio y no se podían facturar los productos adquiridos, situación que era resumida por los empleados del lugar con la sencilla frase "*se cayó la red*"".
- "Al visitar un nuevo mercado inaugurado en la ciudad y al llegar al lugar encontré a una gran cantidad de personas concentradas junto a la puerta de entrada a las que no dejaban pasar bajo el argumento de que no se podía atender al público debido a que "*las cajas se encontraban bloqueadas*" y era imposible cobrar los productos ofertados".
- "Casi todos los que cobran su salario por medio de tarjetas magnéticas en algún momento han visto con desagrado un mensaje en la pantalla del cajero automático donde se anuncia que está "*fuera de servicio por problemas con las comunicaciones*", sin otra opción que dirigirse a otro cajero automático para probar suerte nuevamente o conformarse con no poder utilizar su dinero en el momento deseado".

Circunstancias semejantes a las anteriores se presentan con frecuencia en lugares donde las operaciones se encuentran soportadas en las tecnologías de la información y las comunicaciones. De manera creciente los sistemas informáticos son parte integrante de las rutinas diarias y en consecuencia una interrupción significativa puede tener gran impacto, no solo sobre las personas, sino también en las entidades y provocar pérdidas de todo tipo.

El asunto radica en que con el incremento de la informatización aumenta la dependencia con relación a las tecnologías, de modo que cuando éstas fallan y no se cuenta con alternativas que garanticen la continuidad de las operaciones, fracasan los procesos que dependen de ellas y se presentan situaciones más complejas en procesos críticos asociados a estas tecnologías, tales como los vinculados a la salud de las personas, la actividad industrial o el control del tráfico aéreo, por solo citar algunos, en los que una simple desviación de los parámetros de funcionamiento pudiera provocar terribles consecuencias. [9]

Adicionalmente, la información procesada, contenida y transmitida mediante las tecnologías de la información adquiere características singulares que hacen su protección más compleja, ya que no basta con preservar su disponibilidad para evitar las desagradables situaciones mencionadas anteriormente, sino también se requiere proteger su integridad y su confidencialidad. Su intangibilidad dificulta además mantenerla segura al no poder palparla y supervisarla a semejanza de objetos perceptibles más fáciles de controlar. La falta de información en forma de ceros y unos pasa inadvertida en la mayor parte de los casos. [10]

Con la introducción de las computadoras personales, la cantidad de computadoras empleadas en las entidades creció significativamente, al implantarse muchos más puntos en los cuales los datos y equipos se encuentran expuestos a diversas amenazas.

Cuando los registros dejan de ser tratados en papel y pasan a ser grabaciones de datos en soportes magnéticos surgen nuevas posibilidades de fraude y puesto que los cálculos y asientos son hechos por programas, el delito se hace posible si el malversador puede modificar dichos programas adecuadamente. Por otro lado, la concentración de los datos es cada vez mayor, de manera que en uno o dos minutos se puede extraer información equivalente a cientos de páginas de texto y copiarla a un pequeño soporte muy difícil de detectar. [11]

Quizás alguien podría suponer que este es un tema que concierne solo a los directivos y funcionarios, mientras que otros consideran que es un asunto de los especialistas de la informática o en última instancia de los que se encargan de la seguridad y protección. Pudiera pensarse que siempre habrá alguien para asumir estos problemas, pero en realidad todo el que de alguna forma se encuentre relacionado con las tecnologías de la información de alguna manera se verá involucrado con su seguridad.

La realidad es que los asuntos relativos a la seguridad de las tecnologías de la información son percibidos de forma distinta en dependencia de la posición de cada cual y con frecuencia los criterios dependen del "*cristal con que se mira*", de manera que los directivos esperan de la seguridad informática que los procesos fundamentales de la organización que dirigen no se vean interrumpidos; los funcionarios desean que las aplicaciones y servicios que utilizan para su trabajo no se detengan; los especialistas de informática aspiran a que la red y los equipos terminales no fallen; el personal encargado de la seguridad y protección pretende evitar el robo de equipos y componentes y la fuga de información; los auditores tratan por todos los medios de disminuir la probabilidad de fraudes y los que cuentan con una computadora en su casa aspiran a que les dure eternamente. Por otra parte, algunos creen que la seguridad informática consiste en protegerse adecuadamente de los virus y otros programas maliciosos e incluso hay quien considera que su objetivo se concentra en evitar el acceso del personal a sitios

inadecuados o el envío de correo electrónico al extranjero. Aunque todos tienen algo de razón, la seguridad informática es mucho más que lo descrito. [12]

El término seguridad proviene de la palabra "seguritas" del latín y en una acepción general es sinónimo de "estar seguro". Normalmente se suele definir la seguridad como la ausencia de riesgo o también a la confianza en algo o alguien. No obstante, el término puede tomar diferentes sentidos según el área o campo a la que haga referencia. [8]

La seguridad informática se orienta a la protección de la infraestructura computacional y todo lo relacionado con ésta (incluyendo la información contenida). Para ello existen normas, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información.

Hay tres principios o aspectos fundamentales vinculados con la seguridad informática: la *confidencialidad*, la *integridad* y la *disponibilidad*. [2]

La *confidencialidad*, a veces denominada secreto o privacidad, es la condición, que asegura que la información no pueda estar disponible o ser descubierta por personas, entidades o procesos no autorizados.

Se entiende por *integridad* la condición que garantiza que la información solo puede ser modificada, incluyendo su creación y borrado, por el personal autorizado. Garantiza que la información sea exacta y completa y que el sistema no modifique o corrompa la información o permita que alguien no autorizado lo haga.

La *disponibilidad* es la propiedad que garantiza el acceso a los activos de información y el empleo de los recursos informáticos en cualquier momento por las personas autorizadas. Un sistema seguro debe mantener la información disponible para los usuarios. Disponibilidad significa que el sistema, tanto hardware como software, funciona de forma eficiente y que es capaz de recuperarse rápidamente en caso de fallo.

El enfoque de la seguridad y de los mecanismos utilizados para su implementación está influido en cada caso por el más importante de esos tres aspectos en el lugar de que se trate. De acuerdo al tipo de sistema informático instalado y de las características propias del lugar, el orden de importancia de estos tres factores es diferente, e incluso entran en juego otros elementos como la autenticidad o el no repudio. [2]

Aunque se suele utilizar indistintamente los términos seguridad informática y seguridad de la información se diferencian en que el primero se circunscribe a la seguridad en el ambiente informático, mientras que la información puede encontrarse en diferentes medios y formas y no solo en los medios informáticos. [13]

Queda clara la importancia de la seguridad informática, tanto para directivos, a quienes corresponde la máxima responsabilidad de organizar la política y estrategia de uso y preservación de todos estos procesos informativos y tecnológicos tan requeridos en la toma de decisiones de la esfera que dirigen; funcionarios que operan tanto las tecnologías como la información en ellas contenidas, especialistas de informática a los que corresponde garantizar el soporte seguro donde operan estas técnicas; el personal encargado de la seguridad y protección que garantiza que se cumplan las políticas, medidas y contramedidas empleadas para asegurar los medios, repositorios e información misma. En fin a todo usuario, bien sea una persona jurídica o natural que disponga, y utilice información, soportada en medios tecnológicos, ya sea en red o no.

**Amenazas, riesgos y vulnerabilidades.** [2, 14-16]

Un aspecto que el directivo y todos los factores involucrados en la seguridad informática deben identificar y gestionar son las amenazas, riesgos y vulnerabilidades a los que está sometido el sistema informático.

A diario se enfrentan amenazas y riesgos que por costumbre no se aprecian, aunque se valoran con el propósito de asumirlos o tomar medidas para mitigarlos. Así por ejemplo, antes de salir a la calle para comenzar la jornada de cada día, se valora el estado del tiempo, si hará frío o calor, si lloverá o no lloverá y sobre esta base se estima la probabilidad de ocurrencia de esos eventos meteorológicos y se decide emplear ropa ligera o abrigada, sombrilla o capa de agua e incluso el tipo de zapatos utilizar.

Eventos como los acabados de mencionar, que pueden ocurrir o no, son llamados *amenazas*, la probabilidad de que ocurran las amenazas se denomina *riesgo* y las acciones que se toman para mitigarlos se conocen como *contramedidas* o simplemente medidas.[2, 10, 12-16]

La *amenaza* es una potencial violación de la seguridad y se refiere a una situación o acontecimiento que puede causar daño a los bienes informáticos; indica posibilidad de que algo puede suceder y tiene un carácter cualitativo. Es un factor que incide negativamente sobre las debilidades del sistema y generalmente se describe en función de su origen o de sus posibles consecuencias.

El *riesgo* cuantifica la probabilidad de que una amenaza se materialice, y cause daño (impacto) a los bienes informáticos. Indica cuan probable es una amenaza y se expresa en valores numéricos generalmente entre cero y uno, cero cuando no es posible que la amenaza se produzca y uno si hay certeza absoluta de su materialización.

La siguiente situación que se ha presentado ocasionalmente en nuestro país es una muestra de ello: las computadoras que se encuentran en viviendas y entidades de un área determinada están expuestas a la amenaza de que se produzca un fallo de energía eléctrica, pero algunas de ellas puede que compartan el circuito con un importante hospital y por ello rara vez falta la electricidad por estar priorizado en el sistema de distribución, mientras que otras radican en una zona, donde debido al exceso de consumidores que forman parte del circuito, los fallos de energía se producen con gran frecuencia. Se puede apreciar que aunque todas están sometidas a la misma amenaza (fallo de energía eléctrica) la probabilidad de que esto ocurra (riesgo) es muy baja en el primer caso, tal vez menos de 0,3 y muy alta en el segundo, posiblemente mayor de 0,7.

En dependencia de cómo se originan las amenazas se pueden clasificar en accidentales o intencionales. Las amenazas accidentales pueden deberse a causas naturales, laborales o sociales y se incluyen entre ellas las provocadas por desastres naturales, tales como intensas lluvias e inundaciones, tormentas eléctricas severas o terremotos y aquellas causadas por condiciones medioambientales adversas, como altas temperaturas, elevada humedad y presencia de polvo.

Las amenazas intencionales son provocadas por personas que pretenden acceder o dañar el sistema con motivos y objetivos diversos y como la palabra lo indica tienen lugar de manera deliberada. Una amenaza intencional cuando se materializa se considera una agresión o ataque. Estos ataques pueden ser internos, si los usuarios legítimos de un sistema actúan de forma no autorizada o externos, que se producen frecuentemente con el empleo de las posibilidades de acceso remoto destinadas a usuarios autorizados.

También se entiende por *vulnerabilidad* el punto o aspecto de un sistema que es susceptible de ser atacado o de ser dañada la seguridad del mismo. Representan las debilidades o aspectos falibles o atacables en un sistema informático.

Existen muchos tipos de vulnerabilidades, destacándose entre ellas las físicas y ambientales, que determinan el grado en que el sistema puede verse afectado por desastres naturales o situaciones adversas del entorno; las vulnerabilidades propias de equipos y programas, pues ciertos fallos o debilidades facilitan el acceso a los mismos y los hacen menos seguros y las vulnerabilidades humanas, derivadas de las acciones realizadas por el personal que administra o emplea los sistemas.

Al establecer las medidas de seguridad se debe considerar cual será el costo que se está dispuesto a asumir por cada medida a implantar, pues éstas siempre tienen un costo. Si se considera alta la probabilidad de lluvia y se decide salir con un paraguas, hay que cargar con él durante todo el día (costo) aun incluso si no llega a llover. Otra alternativa podría ser obviar el paraguas y enfrentar la probable lluvia, con lo que se asume el riesgo y este es otro caso donde puede existir un fuerte aguacero y es probable enfermar de gripe. Decisiones como las descritas se basan en una relación definida como costo – beneficio y lo que se persigue es lograr un equilibrio entre ambos criterios, o mejor aún, obtener el máximo beneficio con un mínimo de costo.

El costo de las medidas de seguridad puede expresarse en una mayor complejidad del empleo de las tecnologías, poca funcionalidad de los sistemas, operación más complicada de los equipos, mayor desembolso financiero, retraso en la obtención de los resultados esperados y excesiva dificultad en la comprensión de los procesos, lo que puede ser compensado por beneficios tales como una elevada confianza en la correcta ejecución y eficacia de las operaciones, la certeza de la precisión de los resultados, un adecuado control de acceso, la compartimentación apropiada del empleo de los recursos, la delimitación de responsabilidades y la posibilidad de prevenir, detectar y responder los incidentes de seguridad.

Otro aspecto importante a considerar es la percepción que se tenga de los riesgos, pues existe diferencia entre el riesgo real y el riesgo que se percibe, y esto provoca que de forma reiterada los riesgos no se aprecien de una manera correcta, lo que impide adoptar medidas efectivas para mitigarlos.

Sucede con gran frecuencia que por una u otra razón no se es consciente del riesgo que se corre ante determinadas situaciones y por lo general se tiende a subestimar o hasta despreciar los riesgos existentes al enfrentar situaciones habituales y si ocasionalmente no pasa nada llega el momento en se hace costumbre y se pierde el sentido del peligro. Incide en esto la ignorancia y el desconocimiento que impide valorar una determinada eventualidad, por lo que no se realiza acción alguna para mitigar el impacto que puede producirse como resultado de la materialización de una amenaza.

Un aspecto importante en una institución informatizada en mayor o menor grado es el análisis de riesgos, su gestión y las técnicas para su manejo.

### ***Análisis de riesgos***. [17]

Hay dos aspectos que se pueden diferenciar en el proceso de análisis de riesgos:

1) La *Evaluación de Riesgos* orientada a determinar los sistemas que, en su conjunto o en cualquiera de sus partes, pueden verse afectados directa o indirectamente por amenazas, para lo cual se valoran los riesgos y establecer sus niveles a partir de las posibles amenazas, las vulnerabilidades identificadas y el impacto que puedan causar a la entidad. Consiste en el proceso de comparación del riesgo estimado con los criterios de riesgo, para así determinar su importancia.
2) La *Gestión de Riesgos* que implica la identificación, selección, aprobación y manejo de los controles a establecer para eliminar o reducir los riesgos evaluados a niveles aceptables, con acciones destinadas a:

a) Reducir la probabilidad de que una amenaza ocurra.

b) Limitar el impacto de una amenaza, si ésta se manifiesta.

c) Reducir o eliminar una vulnerabilidad existente.

d) Permitir la recuperación del impacto o su transferencia a terceros.

La gestión de riesgos conlleva la clasificación de las alternativas para manejar los riesgos a que puede estar sometido un bien informático dentro de los procesos en una entidad. Implica una estructura bien definida, con controles adecuados y su conducción mediante acciones factibles y efectivas. Las principales técnicas de manejo del riesgo son las siguientes:

1. Evitar: Impedir el riesgo con cambios significativos en los procesos por la mejora, rediseño o eliminación, como resultado de controles y acciones realizadas.
2. Reducir: Si el riesgo no puede evitarse por dificultades de tipo operacional, la alternativa puede ser su reducción hasta el nivel más bajo posible. Esta opción es la más económica y sencilla y se consigue al optimizar los procedimientos y con la implementación de controles.
3. Aceptar: Asumir el riesgo y tomar las medidas adecuadas para afrontar sus consecuencias.
4. Transferir: Es buscar un respaldo contractual para compartir el riesgo con otras entidades, por ejemplo alojamiento, hospedaje, externalización de servicios, entre otros. Esta técnica se usa, ya sea para eliminar un riesgo de un lugar y transferirlo a otro, o para minimizar el mismo.

Una vez que los riesgos de seguridad han sido identificados y se ha asignado un valor cualitativo a cada uno de ellos, como pudiera ser alto, medio y bajo, el siguiente paso es determinar como tratar ese riesgo. Los procesos de gestión de riesgos generalmente son diferentes en cada tipo de organización.

En función del nivel de impacto esperado y la probabilidad de los riesgos se determina cuan crítica podría ser la situación como resultado de cada riesgo. Este análisis posibilita establecer la jerarquía o prioridades de procesos, sistemas y equipos, permite crear una estrategia que facilita la toma de decisiones acertadas y efectivas, encauzar el esfuerzo y los recursos en áreas donde sea más importante o necesario mejorar la confiabilidad operacional en base a la situación existente. Por ejemplo, una organización puede decidir *aceptar* los riesgos que por su probabilidad e impacto son bajos, *mitigar o reducir* los riesgos que tienen alta probabilidad y bajo impacto mediante la aplicación de medidas de seguridad, *transferir o compartir* los riesgos que son de baja probabilidad y alto impacto hacia un tercero por medio de acuerdos contractuales, y *evitar* los riesgos que tienen una alta probabilidad e impacto por dejar de implementar funciones que impliquen la adopción de tecnologías de alto riesgo.

Para garantizar un enfrentamiento adecuado a las contingencias de seguridad que se presenten, se implementan un conjunto de controles que deben quedar explícitos en el Plan de Seguridad Informática de cualquier institución.

**Implementación de controles**. [2, 17]

Resulta evidente que los beneficios que se derivan del empleo de las tecnologías de la información sobrepasan en buena medida los inconvenientes y riesgos que a su vez traen asociados, razón por la cual éstas son aceptadas y no se discute la necesidad de su utilización. El asunto por tanto radica, no en descartar el empleo de estas tecnologías, sino en conocer cuáles son sus riesgos potenciales con el

objetivo de minimizarlos a través de las políticas, medidas y procedimientos que garanticen un nivel aceptable de seguridad.

Antes de considerar cómo deben ser tratados los riesgos que han sido identificados, se deberán decidir los criterios para determinar si pueden ser aceptados o no. Un riesgo puede ser aceptado, si por ejemplo, se determina que es bajo o que el costo para tratarlo sobrepasa el gasto derivado de sus posibles efectos.

Para cada uno de los riesgos que se identifiquen se tomará una decisión sobre la manera en que se tratará, ya sea por la eliminación de las posibles causas que los propicien, la aplicación de controles apropiados para reducirlos, su transferencia a terceros especializados en su control o la aceptación de manera consciente y objetiva siempre que satisfagan claramente la política y los criterios definidos al respecto.

La decisión acerca de las opciones a considerar deberá tener en cuenta la probabilidad del riesgo, su severidad, el costo de tratarlo y la efectividad de los controles disponibles.

Para aquellos riesgos donde se decida aplicar controles apropiados, estos se seleccionarán e implantarán para lograr los requisitos identificados mediante la evaluación de riesgos. Los controles deben asegurar que los mismos son reducidos a un nivel aceptable.

Durante la selección de los controles de seguridad se tendrá en cuenta el costo de cada control con respecto al riesgo que se quiere reducir, con el fin de lograr que exista un equilibrio entre esos factores, o sea, que no se escatimen recursos pero tampoco se malgasten, mediante la aplicación del principio de proporcionalidad.

La seguridad informática se logra mediante la implantación de un conjunto adecuado de controles, que incluyen políticas, procesos, medidas, procedimientos, estructuras organizativas y funciones de hardware y software.

A continuación se explican las políticas y a las medidas y procedimientos de seguridad informática.

### *Políticas de seguridad*

Comenzar con la definición de las políticas de seguridad a partir de los riesgos estimados debe asegurar que las medidas y procedimientos proporcionen un adecuado nivel de protección para todos los bienes informáticos.

Las políticas de seguridad determinan de qué manera serán empleadas las tecnologías de informática y comunicaciones para aprovecharlas con la mayor eficiencia y seguridad posible. Lo mismo sea una organización grande o pequeña, un comercio o una casa, definir lo más temprano posible las pautas que regirán la utilización de los medios informáticos resultará altamente saludable. Por ejemplo, en una entidad, la definición sobre la custodia y responsabilidad de cada activo informático deberá garantizar que se pueda exigir responsabilidad ante un posible daño o extravío y de igual modo en una computadora domestica dejar claro quien tiene acceso a ella siempre será beneficioso.

Las políticas establecen las normas generales que debe cumplir el personal que participa en el sistema informático y se derivan de los resultados obtenidos en el análisis de riesgos de la institución y de las pautas definidas por las instancias superiores en las leyes, resoluciones, reglamentos y otros documentos rectores.

Las políticas de seguridad conforman la estrategia general. Las medidas y procedimientos establecen en detalle los pasos requeridos para proteger el sistema informático; No pueden haber medidas y procedimientos que no respondan a una política, al igual que no puede concebirse una política que no esté complementada con las medidas y procedimientos que le correspondan.

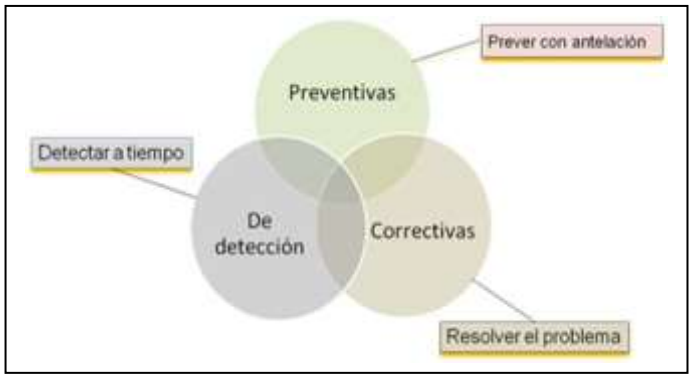
Una buena política de seguridad debe poder implementarse a través de medidas y procedimientos; el establecimiento de principios de uso aceptable u otros métodos apropiados; poder hacerse cumplir por medio de herramientas de seguridad, donde sea conveniente y definir claramente las responsabilidades de cada una de las personas con acceso a los sistemas y sus servicios.

***Medidas y procedimientos***

Usualmente se intenta mantener el orden de las acciones a realizar para garantizar que nada quede por hacer ni sea olvidado. De lo que se trata es de sistematizar su realización para que todo sea más fácil, no se omita ningún detalle y se logren los resultados deseados.

Las medidas y procedimientos para la protección de un sistema informático se definen a partir de la identificación de los posibles eventos que puedan causar la interrupción o afectación de los procesos y considerarán básicamente las acciones a realizar; la determinación de las responsabilidades de su cumplimiento y los recursos necesarios en cada caso.

En correspondencia con el momento de su aplicación las medidas y procedimientos pueden ser *preventivas*, orientadas a adelantarse a la materialización de una amenaza mediante acciones dirigidas a evitarlas o a minimizar el impacto de las mismas, de *detección*, dirigidas a identificar y descubrir a tiempo los eventos que puedan producirse o *correctivas,* que intentan resolver los problemas ocasionados.




**Tipos de medidas y procedimientos**

De acuerdo con su naturaleza también pueden ser físicas, lógicas, organizativas, legales o educativas.

Como regla un solo tipo de medidas no es suficiente. Se necesita examinar el "nivel aceptable de pérdidas" y tomar una decisión acertada, por lo que se debe combinar adecuadamente medidas de diferentes tipos, a partir de la identificación de las amenazas potenciales sobre el sistema y la definición de los controles a aplicar bajo la consideración de criterios de costo – beneficio.

Existen cuatro razones básicas para implantar una medida de seguridad:

a) La medida es obligada por la ley o por las regulaciones vigentes.

b) El costo es mínimo, pero los beneficios son significativos.

c) Su implementación impedirá una perdida infortunada a un costo tolerable.

d) La medida de seguridad puede ser justificada en costos.

Las dos primeras razones deben ser tenidas en cuenta de inmediato sin consideraciones futuras y para las dos últimas es preciso realizar un análisis de costo beneficio.

Debido a que cada sistema informático es una combinación única de amenazas y bienes, ningún grupo de controles es óptimo para todas las entidades y por lo tanto es imprescindible su establecerlo de forma diferenciada en cada lugar con criterios rentables a partir de un análisis de riesgo para identificar los bienes más expuestos.

Muchos controles de seguridad, en particular los que corresponden a procedimientos de operación, se pueden aplicar a muy bajo o ningún costo y si van a tener un impacto significativo que evite pérdidas futuras se pueden aplicar sin una detallada justificación de costos.

Las medidas y procedimientos en una organización deben especificar en detalle lo que hay que hacer, cómo y cuándo hacerlo, que recursos requieren emplearse y quienes participan en su realización, pues al contrario de las políticas generales que están destinadas para toda la entidad, ellas son específicas en función de las necesidades de cada área.

**Conclusiones**

El tema tratado es de gran importancia para directivos, funcionarios, especialistas de informática, seguridad y protección de la informatización en las instituciones de salud pública y en general de todas aquellas que se incluyen en el proceso social actual y hace énfasis en:

- Los principios fundamentales de la seguridad informática: confidencialidad, integridad y disponibilidad
- La percepción e identificación de amenazas, riesgos y vulnerabilidades del sistema informático.
- El análisis de riesgos para definir políticas, medidas y contramedidas que garanticen el costo – beneficio del sistema Y que permita aceptarlos, mitigarlos, reducirlos, transferirlos o compartirlos y evitarlos.
- Las políticas de seguridad como estrategia general, que aseguren las medidas, contramedidas y procedimientos que respondan a esas políticas y contengan los pasos requeridos para proteger el sistema informático.

Si no se percibe de manera adecuada el riesgo no se puede enfrentar. Por tanto, lo primero que se debe hacer es identificar los riesgos a que se enfrenta el sistema informático institucional, evaluarlos minuciosamente y gestionarlos de manera adecuada con el fin de evitarlos, mitigar sus efectos o aceptarlos tomando las medidas adecuadas para afrontar sus consecuencias.

## REFERENCIAS BIBLIOGRÁFICAS

1. Gay A. La tecnología y la historia. [Internet]. [citado 8 Dic 2015]. Disponible en: http://www.ifdcelbolson.edu.ar/mat_biblio/tecnologia/curso1/u1/05.pdf
2. García Pierrat G. Seguridad Informática. La Habana: G.L.D; 2003.
3. Salazar CM. Disposición frente al cambio tecnológico: Un estudio empírico [Internet]. Chillán (Chile): Universidad del Bío-Bío; 2002 [citado 8 Dic 2015]. Disponible en: http://www.panorama.utalca.cl/dentro/2004-oct/3.pdf
4. Prensky M. Digital natives, digital immigrants. On the horizon [Internet]. 2001 [cited 18 Dec 2015]; 9(6): 1-9. Available from: https://edorigami.wikispaces.com/file/view/PRENSKY%20-%20DIGITAL%20NATIVES%20AND%20IMMIGRANTS%202.PDF/30785667/PRENSKY%20-%20DIGITAL%20NATIVES%20AND%20IMMIGRANTS%202.PDF
5. Piscitelli A. Nativos e inmigrantes digitales. ¿Brecha generacional, brecha cognitiva, o las dos juntas y más aún?. Rev. Mexicana de Investigación

Educativa [Internet] 2006 Ene-Mar [citado 8 Dic 2015]; 11(28): 179-85. Disponible en: http://www.redalyc.org/pdf/140/14002809.pdf

6. García Pierrat G. Ingeniería Social. Revista PuntoCU. 2003
7. Norma cubana NC/IEEC 17799: Código de buenas prácticas para la gestión de la seguridad de la información. 2007
8. Avogadro M. Seguridad y nuevas tecnologías: un binomio necesario [Internet] [citado 18 Dic 2015]. Disponible en: http://www.forodeseguridad.com/artic/miscel/6100.htm
9. Vidal Ledo M, García Pierrat G. Seguridad, información y salud. Revista Cubana de Informática Médica [Internet]. 2005 Ene-Mar [citado 18 Dic 2015]; 1(5). Disponible en: http://www.cecam.sld.cu/rcim/revista_7/articulo_htm/segurinfsalud.htm
10. García Pierrat G. La Seguridad Informática como componente de la Seguridad y Protección. La Habana: Dirección de Protección, MININT; 2001.
11. García Pierrat G. El delito en tiempos de Internet. XI Encuentro Internacional Ciencias Penales [CD-ROM]. La Habana: Fiscalía General de la República; 2012.
12. Oficina de Seguridad para las Redes Informáticas. Metodología para la Gestión de la seguridad informática (proyecto) [Internet]. La Habana: OSRI; 2013 [citado 19 Dic 2015]. Disponible en: http://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf
13. Dunn MA. A Comparative Analysis of Cybersecurity Initiatives Worldwide [Internet]. Zurich: Swiss Federal Institute of Technology; 2005 [cited 18 Dec 2015]. Available from: http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf
14. Brownlee N, Guttman E. RFC2350: Expectations for Computer Security Incident Response [Internet]. RFC; 1998 [cited 11 Dec 2015]. Available from: http://www.ietf.org/rfc/rfc2350
15. ISO/IEC 18044: Information technology -- Security techniques -- Information security incident management [Internet] 2004 [cited 16 Dec 2015]. Available form: http://www.iso.org/iso/catalogue_detail.htm?csnumber=35396
16. West-Brown MJ, Stikvoort D, Kossakowski KP, Killcrece G, Ruefle R, Zajicek M. Handbook for Computer Security Incident Response Teams (CSIRT´s). 2nd Ed [Internet]. Pittsburgh, PA: Carnegie Mellon University; 2003 [cited 11 Dec 2015]. Available form: ftp://ftp.sei.cmu.edu/pub/documents/98.reports/pdf/98hb001.pdf
17. García Pierrat G. Administración de incidentes de Seguridad Informática. 2014.

Recibido: 2 de enero de 2016.
Aprobado: 6 de enero de 2016.

*Lic. Gonzalo García Pierrat*. Oficina de Seguridad para las Redes Informáticas. Cuba
Correo electrónico: gonzalo@osri.gov.cu