

INSEGURIDAD INFORMÁTICA Y CIBERCRIMEN¹

- mito y amenaza -

Prof. Arnoldo Moreno Pérez
miru@prodigy.net.mx
arnoldo_58@hotmail.com
amorenop@ipn.mx

Para Aurora López Carmona y *Mirushka*, por ser razón e inspiración de mi vida.

Resumen: Este libro tiene como propósito asumir un punto de vista en torno a la situación actual de la seguridad de los sistemas, puntualizando algunas alternativas para construir un futuro, deseable, factible y probable, que redunde también en algo benéfico para la seguridad humana y social del planeta mismo. Lo anterior como consecuencia de la construcción de mundos virtuales más seguros, donde la propuesta es equilibrar la lucha legítima en contra del terrorismo cibernético y el derecho inalienable de los ciudadanos a la privacidad.

INTRODUCCIÓN

Este trabajo no pretende ser la panacea, en relación al título que ostenta, pero sí algo novedoso y emprendedor. Aspiramos a romper paradigmas orientando de manera responsable al lector hacia un conocimiento imparcial de los virus y antivirus en primera instancia, como eje rector inicial de la problemática que nos ocupa.

El asunto de la seguridad de los sistemas, es –de hecho- inseguridad informática, en todo el sentido de la palabra. Incluso, en lo que concierne a la seguridad como término genérico,

¹ El autor desea expresar todo su respeto, gratitud y reconocimiento a varias personas que han influido en su formación: Bernardo Quintero (HISPASEC), Ignacio Miguel Sbampato (VIRUSATTACK), José Luis López (VSANTIVIRUS), Marcelo Maciel Sosa (SEGURIDAD Y DEFENSA), Mercè Castells (EMPRENDEDORAS), Christian Borghello (SEGU-INFO), Mario Andrés García López, José Anaya Pedrero (CIBERSEL), Juan Carlos Zampatti Maida (ZAMPATTI MAIDA Y ASOCIADOS), Vicente Coll (ONTINET), Anton Zajac (ESET), Carlos Soto, Jorge Alberto Lizama Mendoza, Arturo Guillemaud Rodríguez Vázquez, Miguel Ángel Pérez Wong, Martha Silva Antonio, Eugenia Soria López, Juan Carlos Cruz Moreno, Felipe Chao Ebergenyi y muchas personas más.

carece de sentido el término mismo; no podemos eliminar los riesgos sino solamente disminuirlos o prevenirlos. La primera regla de oro, es el sentido común para no exponerse a riesgos innecesarios, aunada a una capacitación gradual y constante sobre el tema.

El segundo punto a considerar es el delito informático, y una buena aproximación que nos permita entender cómo nace y se manifiesta el crimen cibernético, considerando sus alcances reales.

Las empresas de Antivirus y Seguridad Informática, suelen hacer pronósticos sobre los eventos venideros en el campo de los códigos maliciosos a corto plazo, caracterizándose por un enfoque completamente determinista, aunque no por ello superficial ni carente de validez. Lo verdaderamente importante, es entender el juego de actores que inciden en el mundo de la inseguridad informática y del “cibercrimen”, como se relacionan entre sí, y los escenarios que pueden darse en el corto, mediano y largo plazo.

Se trata de hacer prospectiva (*prospective*) más que pronóstico (*forecasting*), sobre el tema. Buscamos escudriñar cómo construir el futuro, en vez de adivinarlo o preverlo. Esto es, ir más allá y no solamente anticiparse. Trabajaremos en tres etapas: Estudio del futuro (temas de prospectiva); Códigos maliciosos (poniendo énfasis en la problemática de los virus y antivirus), y finalmente -antes de las conclusiones- en el diagnóstico y alternativas de prevención de la inseguridad informática y el crimen cibernético (“cibercrimen”).

ÍNDICE

I. Estudio del futuro.

I.1.- Pensar el futuro..., y construirlo

I.1.1.- Pasado, presente y futuro.

I.1.2.- Prospectiva y estudio del futuro.

I.2.- Pronóstico y Prospectiva

I.2.1.- Diferencia entre pronóstico y prospectiva.

I.2.2.- Métodos y técnicas de pronóstico para intentar visualizar futuros

I.2.3.- Precisiones sobre algunos métodos

II.- Virus y antivirus

II.1.- La génesis y el devenir de los virus informáticos

II.2.- Panorama actual de los distintos antivirus

III.- Cibercrimen

A manera de conclusión

Referencias

Apéndices

Acerca del Autor

I.- ESTUDIO DEL FUTURO.

Reviste una importancia primordial mencionar algunos elementos que permitan dilucidar la importancia de pensar en el futuro y conduzcan a una visión estratégica para tratar de participar de una manera responsable y dinámica en su construcción. Esta ardua tarea es de todos, para todos y con miras al mejor desenlace para la supervivencia de la especie humana y la materialización de un horizonte luminoso de bienestar y tranquilidad para toda la humanidad.

Complementariamente abordaremos de manera clara y sucinta, y a la vez intuitiva –evitando entrar en detalles técnicos tediosos- conceptos tales como *mínimos cuadrados, análisis de regresión, promedios móviles, series de tiempo, método de Box y Jenkins para series temporales*, etc. (de alguna manera haremos referencia a ellos) Remarcando cómo estos conceptos están vinculados a lo que llamamos “*Pronóstico*”, pero que pueden ser útiles en la “*Prospectiva*” en lo que concierne a la evaluación de *futuros probables*.

I.1.- PENSAR EL FUTURO Y CONSTRUIRLO...²

“*El azar solamente favorece a los espíritus precavidos*”. Blas Pascal (1623-1662), matemático, físico y filósofo religioso francés.

“*El futuro no pertenece a los que saben esperar, sino a quienes saben anticiparlo*”. María Espinoza, mexicana campeona mundial de taekwondo.

Vivimos –en pleno siglo XXI- tan sometidos por las urgencias que nos impone el presente que apenas si nos queda tiempo para sobrevolar por encima de las circunstancias y mirar más allá, tratando de escudriñar qué nos depara el tiempo que aún no ha transcurrido (conocido en primera instancia como el *futuro*, ya sea que se le conceptualice como *destino, porvenir o devenir*). Con una especie de infantil insensatez, preferimos ignorar que “inexorablemente” se

² Este capítulo queda íntegramente dedicado a: C. P. Verónica Agustín Domínguez, Lic. Rafael Gerardo Arzate Torres, M. en C. Alba Martínez Olivé, Dr. José Enrique Villa Rivera, Dra. Georgina Zárate Vargas y naturalmente la Lic. Aurora López Carmona (mi esposa). Todos ellos verdaderos profesionales -comprometidos con la construcción de un mejor futuro para México y excelentes personas de quienes he recibido apoyo, aprecio, respeto y consideración.

van a ir produciendo cambios y que el espejismo de nuestra seguridad transitoria podría desvanecerse.

1.1.1.-Pasado, presente y futuro

Estos tres estados o formas en que se nos presenta el tiempo, eclipsando toda nuestra existencia, merecen ser comentados en forma somera e intuitiva como la base para abordar lo que eventualmente se pueda hacer con el futuro.

PASADO	PRESENTE	FUTURO
<ul style="list-style-type: none"> - Tiempo ya transcurrido. - Conjunto de hechos relativos a una persona o colectividad en tiempo anterior al presente. <p><u>Remarcamos:</u></p> <p><i>“El tiempo vuela tan rápido del pasado al futuro que no se detiene ni un instante.”</i> San Agustín (Confesiones).</p> <p><i>“Sólo conservando el pasado aprovechable por medio de la memoria y conquistando el futuro por adelantado por medio de la anticipación, es que el hombre permanece libre.”</i> Paul Fríase (The psychology of time. Londres, 1964, p. 172).</p> <p><i>“... los pueblos se conocen no sólo por su historia, sino también por sus proyectos.”</i> Octavio Paz.</p>	<p>Derivado del latín <i>praesentem</i>, significa:</p> <ul style="list-style-type: none"> - Que está delante o en presencia del que habla, en el mismo lugar que él o en el instante en que está ocurriendo algo. - Tiempo en que actualmente está el que habla o de los acontecimientos que ocurren en él. <p><u>Remarcamos:</u></p> <p><i>“... conformar el futuro es algo que se hace en el presente.”</i> Michel Godet (Creating Futures-Scenario Planning as Strategic Management Tool).</p>	<p>Lo que está por venir o suceder, viene del latín <i>futurum</i>.</p> <p><u>Destino</u></p> <ul style="list-style-type: none"> - <i>Hado, divinidad o voluntad divina que regula de una manera fatal los acontecimientos futuros.</i> - <i>Encadenamiento de los sucesos considerado como necesario y fatal.</i> - <i>Circunstancia o situación a que una persona o cosa ha de llegar inevitablemente.</i> <p><u>Porvenir</u></p> <p><i>Tiempo futuro o situación futura.</i></p> <p><u>Devenir</u></p> <p><i>Palabra que se utiliza en filosofía para expresar el movimiento por el cual las cosas se transforman. Acaecer, llegar a ser o transformarse.</i></p>

A partir de este cuadro, no es difícil sospechar que el futuro no es algo que esté predeterminado de antemano sino algo que se escribe a cada momento con nuestras acciones. Entendemos por prospectiva –según Gastón Berger- “disciplina que estudia el futuro para comprenderlo y poder influir en él”, por ello Miklos y Tello establecen que “la prospectiva se preocupa más por brindar alternativas futuras que por responder a la pregunta: ¿qué sucederá?”³. Hablar de lo que pueda llegar a suceder significa hablar de pronóstico, mientras que mencionar la palabra prospectiva (del latín *prospicio*, ver a lo lejos) es referirnos a lo opuesto al término retrospectiva, que se refiere a dar marcha atrás en el tiempo.

1.1.2.- Prospectiva y estudio del futuro

La prospectiva es la identificación de un futuro probable y de un futuro deseable, diferente de la fatalidad y que depende únicamente del conocimiento que tenemos sobre las acciones que el hombre quiera emprender. Existen dos maneras de tratar de comprender el futuro, estas son: como realidad única, o bien, como realidad múltiple.

Lo han atendido como una realidad única: los adivinos, brujos y charlatanes, los oráculos y todos los que consideran que existe inequívocamente un destino que decide y marca los hechos de la vida, considerándolo como algo inviolable, ciego e inmodificable, negando toda posibilidad a la premisa de que, el hombre es el arquitecto de su propio destino (o sea que, el destino no le es propio y mucho menos puede construirlo o diseñarlo). Para quien cree en el destino, nada deviene, todo está escrito de antemano.

Si concebimos al futuro como una realidad múltiple, explícitamente aceptamos que un hecho del presente puede evolucionar de diversas maneras y llegar a presentarse de diferentes formas. A estos *futuros posibles*, Bertrand de Jouvenel los denominó *futuribles*. Dentro de éstos, los que tienen mayor posibilidad de presentarse, se les llama *futuros probables*, los cuales pueden acontecer con más certeza, no por culpa del destino sino dependiendo de la manera en que el hombre participa en la construcción o diseño del futuro.

³ Miklos, Tomás y Tello, M^a. Elena. ***“Planeación Prospectiva. Una estrategia para el diseño del futuro”***. Editorial Limusa, 2006. Página 21.

Para hablar de futuros probables, en prospectiva se suelen sopesar: la visión de los expertos, el comportamiento de los actores que intervienen y las leyes matemáticas del cálculo de probabilidades. El discurso prospectivo se encamina a identificar la acción futura en base a estos elementos. Cuando este tipo de futuro, no representa lo más positivo, se busca evaluar que este sea probable, pero también deseable.

Tenemos que:

“El futuro siempre ha capturado la atención, el interés y la curiosidad humanos. Desde la antigüedad hasta nuestros días, la percepción humana sobre el porvenir ha transitado por diferentes formas de comprenderlo y enfrentarlo. Para muchas sociedades ha significado miedo y resignación, para otras, la oportunidad de construir caminos diferentes hacia visiones compartidas del porvenir.”⁴

- ¿Qué es lo que hace que pongamos atención al futuro?

Todos tenemos un temor al parecer innato de percatarnos –de antemano- hacia donde se dirigen –quizá inevitablemente- nuestros pasos y si tenemos alguna oportunidad de corregir el rumbo. Y, ¿por qué no?, de saber si finalmente tiene sentido hablar del destino.

- ¿Por qué nos interesa el futuro?

Parece natural, saber si vamos a seguir vivos y cómo será nuestra vida y si podrán cumplirse nuestras ilusiones, aspiraciones y sueños.

- ¿Por qué el futuro es algo que despierta nuestra curiosidad?

Simplemente, saber algo acerca de él, permite *acariciar* la idea de que algún día podremos respondernos –aunque sea de manera parcial o acotada- esa inquietante pregunta que se pierde –y late incesantemente- en la noche de los tiempos: ¿Quiénes somos, de dónde venimos y hacia dónde vamos? (¡Hermosa trenza dorada que concatena pasado, presente y futuro enlazados como los vértices y a la vez el alma que da vida a ese

⁴ Cruz Moreno, Lic. Juan Carlos (2008). ***“PROGRAMA PARA LA ASIGNATURA Prospectiva Estratégica.”*** Facultad de Ciencias Políticas y Sociales (FCPyS) de la UNAM. Página 1.
<http://pensarelfuturo.files.wordpress.com/2008/02/prospectiva-estrategica.pdf>
 (Consultado el lunes 16 de abril de 2008).

bello triángulo de nuestra existencia -siempre vibrante-, cuyos lados son también las tres dimensiones temporales, girando en torno a un círculo cuya naturaleza desconocemos!).

- ¿Cuáles han sido las distintas formas que ha tenido el hombre de comprender y enfrentar el futuro?

Es una historia verdaderamente compleja, no es sencillo pretender un panorama completo y a la vez preciso. Un estudio detallado al respecto, debe incluir las explicaciones históricas y sociológicas que nos conduzcan a entender, cómo es que el hombre se ha involucrado con aspectos y temas tales como: adivinación, oráculos, profecías, ciencia ficción y todo tipo de literatura de índole –quizá- futurista. Se trata de dilucidar dónde hubo visión, coincidencia o solamente fantasía, o incluso burda manipulación de los hechos o de las cosas.

La otra cara de la moneda, nos conduce a valorar lo que se ha logrado conquistar de manera científica, no es lo mismo poder afirmar con seguridad que *el sol volverá a salir mañana* o que en algunos miles de años se extinguirá, a tratar de vaticinar cómo será la sociedad humana del siglo XXXIII. O sí, se quiere ver o dilucidar los aspectos más complicados, sería interesante saber si siempre existe un camino óptimo para intervenir en la construcción del futuro, de tal suerte que nos conduzca al mejor de los futuros, seleccionado entre una gama quizá infinita de escenarios factibles o incluso inesperados. (¡Esto es la locura!... pero a veces la realidad, sobrepasa no solamente a la fantasía sino también a la locura misma: Si no lo creen, pregúntenle a Osama Bin Laden, George Bush, Fidel Castro o Hugo Chávez, dónde han escondido a la cordura, o ¿debemos reconocerlos como locos geniales?... En fin, todo esto es demasiado complicado, impredecible, y la lógica fría inhibe analizarlos –tratando de comprenderlos y explicarlos satisfactoriamente- en términos fenomenológicos o prospectivos).

- Para algunas sociedades, el miedo y la resignación ha estado acompañado de las creencias religiosas. Los aztecas veían en sus profecías un desenlace fatal y sentían que inexorablemente iban hacia la caída de su imperio, tenían claro que no podían modificar su destino ni cambiar la voluntad de sus dioses. El sentimiento trágico de la existencia, constituye la antítesis de la confianza en el futuro como un horizonte luminoso lleno de oportunidades (aunque también de obstáculos).

- En lo que concierne a la oportunidad de construir caminos diferentes hacia visiones compartidas del porvenir, no podemos pasar por alto, la influencia que tuvo Gottlob Fichte –cuando escribió sus célebres “Discursos a la Nación Alemana”- en la formación del “espíritu alemán de grandeza” que orientó en gran medida, el rumbo que tomó el nacionalismo alemán a fines del siglo XIX y principios del XX. Un país que se empieza a interesar por tratar de construir su futuro –independientemente de que consiga tener una visión clara o “acertada” de ello-, comienza a sentar las bases que le permitirán aprender –hasta cierto punto- cómo hacerlo, al menos en determinados aspectos.

“La reflexión sobre el futuro en el campo científico ha sido constante. En las ciencias exactas, la astronomía, la física, la agronomía, la biología, la demografía y la economía se comenzaron a desarrollar métodos cuantitativos y cualitativos que permitieran, sobre la base de hechos presentes y pasados, estimar las probabilidades de ocurrencia de determinados fenómenos. Los estudios sobre el futuro –basados en la extrapolación- se dirigieron a analizar las tendencias del pasado y del presente que les permitieran deducir una idea del porvenir.”⁵

- La ciencia siempre ha sido concebida como un sistema de pensamiento en constante evolución, pasado y presente para la construcción de un mejor porvenir; por ende, el futuro como preocupación siempre ha estado presente.
- Respecto a las ciencias exactas: ¿Qué ciencia puede ser –en realidad- exacta, en un universo tan complicado y lleno de incertidumbre? Esta, es meramente una forma de referirse a las matemáticas y lo que de ellas se deriva.
- Es en el seno de las “ciencias exactas”, donde nacen con “cierta precisión” las nociones que permiten entender lo *determinístico*, *probabilístico* y *aleatorio*, como ingredientes de cualquier fenómeno lo suficientemente complicado, en el que se pretenda establecer algún pronóstico.
- Desde la antigüedad, los babilonios y los mayas tenían claro la naturaleza cíclica de ciertos fenómenos astronómicos, que permitieron la elaboración de calendarios, estimar la duración del día y la noche, la duración de las estaciones del año. Claro está,

⁵ Op. Cit., Ídem.

que en esta clase de eventos, establecer proyecciones acerca de lo que iba a ocurrir con los movimientos de ciertas estrellas, no era algo que para ellos fuese inaccesible.

- En la actualidad, con los grandes telescopios, observamos eventos que ocurrieron hace millones de años, percibiéndolos como hechos del presente. No obstante, estamos conscientes de ello, lo que nos permite mirar hacia el pasado para entender un presente, que cuando lo empezamos a comprender ya es futuro. ¡Qué bella paradoja! ¿Acaso estaremos siempre impedidos para –mediante un recurso tecnológico, propio de una civilización lo suficientemente avanzada- poder ver el futuro o la enorme gama de futuros posibles o admisibles?
- La física, esa gran aventura del pensamiento, cuyos cimientos vienen desde Arquímedes y llegan hasta Albert Einstein y Stephen Hawking, se ocupa del tiempo –y por ende, de paso también del futuro- desde las primeras investigaciones en torno al movimiento de los cuerpos, hasta los estudios de la relatividad del tiempo y del espacio, llegando a tocar actualmente terrenos tan intrincados como las supercuerdas, el campo unificado y los hoyos negros.
- En lo que concierne a la agronomía, desde tiempos inmemoriales el hombre ha ido vislumbrando formas de planear los cultivos y el aprovechamiento del campo, tratando de implementar o planear cosas que le sirvan en un futuro.
- En las ciencias biológicas, el fenómeno de la vida siempre ha ido acompañado de las nociones de pasado, presente y futuro. De manera similar a la astronomía, existen eventos que se dan de manera cíclica o con cierto rango de determinismo. Sabemos que enfermedades son más frecuentes en determinadas temporadas, que no es lógico ni normal que un embarazo pueda durar más de un año en la mujer (¡no sabemos de hombres que se hayan embarazado!), que todos los seres vivos nacemos y morimos (¡el futuro nos depara que algún día seguramente moriremos!). En fin, en la vida, el futuro siempre determina y condiciona ciertos hechos, siendo bastante probable –quizá- que ello ocurra en todos los futuros posibles. (Con ello, no se pretende darle cabida al destino, sino a la presencia de determinados eventos –que aunque puedan presentarse de maneras diversas- no puedan evitarse o revertirse).
- El estudio del crecimiento y las dimensiones de la población, a fin de tener proyecciones que permitan una mejor planeación para lograr establecer todo tipo de

“satisfactores” para los distintos conglomerados humanos, ha sido siempre una preocupación incesante, incluso desde antes de que existiese la demografía, ya configurada y establecida como algo científico. En una ciencia como esta, los pronósticos basados en las llamadas series de tiempo, en ocasiones llegan a tener un grado aceptable de certidumbre, pero no adquieren el rango de un conocimiento científico incuestionable, sino de casualidades fortuitas dignas de destacarse.

- En la economía, el desarrollo de métodos cuantitativos y cualitativos para tratar de tener cierta anticipación a los hechos –o bien un pronóstico verdaderamente útil para la toma decisiones- no ha sido todo lo afortunado que se quisiera. La historia nos marca – más frecuentemente- situaciones en las cuales ha triunfado más una decisión política – a veces visceral o aparentemente irreflexiva- que todo un bagaje técnico minuciosamente preparado para enfrentar las cosas. A menudo, es más eficiente poseer una intuición hacia el carácter social de las relaciones económicas y la razón de ser de los mercados financieros (y su mecánica intrínseca), que creerle a los modelos sofisticados de la econometría y las series de tiempo -los cuales están plagados de ideas radicalmente deterministas para tratar de explicar un mundo real- y otros más que van surgiendo. Llega a ser preferible, vislumbrar lo que puede suceder y cómo cualitativamente incidir para mejorarlo, que poder atinarle al pronóstico del valor del euro frente al dólar dentro de un siglo o dentro de dos días (si no hay sustancia para enfrentarse radicalmente y cambiar el mundo, no nos sirven de mucho las cantidades precisas o hasta incluso desglosadas).

“...sería hasta después de la Segunda Guerra Mundial cuando el estudio del futuro se constituye como disciplina académica. La creación, en 1945, de la Fundación RAND (Research and Development) en los Estados Unidos, y el movimiento prospectivo en Francia encabezado por Gastón Berger que culmina con la fundación del Centro Internacional de Prospectiva en 1957, capturaron el interés de múltiples especialistas en diversos campos del saber humano por explorar el porvenir y alertar a la sociedad de los peligros y oportunidades

que ahí se esconden. Precisamente, durante estos años, Ossip Flechtheim acuñó el término “futurología” para referirse a la interrogación sistemática y organizada del devenir.”⁶

- De acuerdo con *Larousse*, futurología es el “conjunto de investigaciones que estudian el futuro e intentan prever cuál será, en un momento dado, el estado futuro del mundo o de un país en los campos social, político, etc.”⁷
- De Gastón Berger, conviene retomar en estos momentos, varias de sus premisas expresadas en le *Revue Prospective* núm. 1 de 1958 (conforme a la traducción de Eduardo Hernández González para la Universidad de Guadalajara⁸), al referirse a la actitud prospectiva, pues son un buen aperitivo para la reflexión profunda de estos temas. Transcribimos textualmente:

“Más que un método o una disciplina, la prospectiva es una actitud, es decir, el adjetivo debe preceder al sustantivo.

El sentido del término "prospectiva" es evidente y está formado de la misma manera que el de "retrospectiva"; ambos se oponen en la medida en que el primero expresa que miramos hacia delante y no hacia atrás. Un estudio retrospectivo se dirige hacia el pasado y el prospectivo hacia el futuro.

Estos dos adjetivos no son perfectamente simétricos en cuanto a su significado, pero sí en su forma, porque tendemos de manera habitual a representarnos el tiempo como una línea en la que el pasado y el futuro corresponden a las dos direcciones posibles. En realidad, el ayer y el mañana son heterogéneos. En cuanto al primero, sólo podemos visualizarlo porque ya no hay nada que podamos hacer, mientras que el mañana significa proyectos cuyas posibilidades están abiertas. Pasar de la retrospectiva a la prospectiva no implica sólo reorientar la atención; requiere una preparación para la acción”.

⁶ Op. Cit., Ídem.

⁷ “**Larousse diccionario enciclopédico usual.**” Tercera edición (2007). Ediciones Larousse, S.A. de C.V., Londres núm. 247, México 06600, D. F. Página 318.

⁸ Berger Gastón. “**La actitud prospectiva.**” (2002). Dossier: Futuro y prospectiva. Revista Universidad de Guadalajara. URL: http://mail.udgvirtual.udg.mx/biblioteca/bitstream/20050101/898/1/La_actitud_prospectiva.pdf (Consultado el lunes 16 de abril de 2012)

- Es importante –en la medida en que, logremos involucrarnos en el quehacer de la Prospectiva Estratégica- remarcar que:

“Debemos comunicar el futuro porque no somos nosotros quienes debemos dar solución a toda la maraña universal en que vivimos. Cada individuo, desde su contexto puede asumir un compromiso individual, comunitario y local con visión global. El problema esencial del futuro es la comunicación, es decir, cómo es que podremos transmitir en forma responsable a cada uno de los demás lo que puede y no acontecer, el futuro no es de unos cuantos, todos llegaremos a él y todos debemos movilizar nuestros esfuerzos para lograr escenarios futuros satisfactorios que nos alejen de lo funesto.”⁹

Aunado a esto:

“... el futuro no es algo único y predecible, por el contrario, es un espacio abierto donde se puede construir la voluntad del hombre. Así, rompe con otras formas de ver el futuro como algo establecido donde la acción del hombre no tiene mayor influencia para cambiarlo, y por lo tanto es predecible, tal como lo establece la adivinación, la profecía, la astrología, e incluso la ciencia ficción, que son estudios del futuro que no pretenden construirlo, sino en contra parte, adivinarlo, predecirlo, imaginarlo o, en todo caso, soñarlo desde el punto de vista de la utopía.”¹⁰

Deliberadamente no quise llevar las cosas por el lado de la confrontación con Fukuyama y lo que llama el fin de la historia, ni tampoco polemizar sobre la visión hegemónica del imperio, de construir el futuro de toda la humanidad en base a sus intereses.

⁹ Rodríguez Vázquez, José de Jesús. **“EL FUTURO AYER Y LA PROSPECTIVA HOY, PARA EL MAÑANA”**. URL:

<http://catedradh.unesco.unam.mx/catedradh2007/SeguridadHumana/prospectiva%206/revista/numero%203/construf/conspira/jesus.htm> (Consultado el lunes 16 de abril de 2012).

¹⁰ Pérez Wong, Miguel Ángel. **“QUÉ ES LA PROSPECTIVA? DEL MITO A LA REALIDAD SOBRE LA CONSTRUCCIÓN DEL FUTURO”**.

URL:

<http://catedradh.unesco.unam.mx/catedradh2007/SeguridadHumana/prospectiva%206/revista/numero%203/construf/conspira/wong.htm> (Consultado el lunes 16 de abril de 2012).

Para mi es claro que el futuro es un espacio abierto, aderezado por un horizonte luminoso de posibilidades y que todos los seres humanos –como especie pensante- podemos participar de manera profunda, dinámica e interactiva en su construcción.

Definitivamente vale la pena pensar en el futuro, para todos, por el bienestar de todos y para consolidar cada vez más la gloria del espíritu humano. ¿Cómo?... lo sepamos o no, o participamos u otros construirán nuestro futuro acorde a sus intereses y tal vez ni tomemos consciencia de ello.

Seamos partícipes y de ser posible hasta protagonistas preclaros en el ejercicio de esa maravillosa “indisciplina” llamada prospectiva estratégica... Pues:

*“... le future ne se prévoit pas, il se construit (... el futuro no se **predice** sino se construye).”*
Maurice Blondel.

I.2.- PRONÓSTICO Y PROSPECTIVA

“El futuro no sólo se prevé... se concibe, se prepara, se diseña y se construye”. Tomás Miklos.

“El futuro no depende necesariamente del pasado, sino exclusivamente de la acción del hombre, las cosas sucederán no tanto porque así lo determinen las leyes matemáticas de la probabilidad, sino porque hemos podido identificar cual va a ser la voluntad del hombre, único responsable de su propio destino”. Gaston Berger y Bertrand de Jouvenel.

I.2.1.- Diferencia entre pronóstico y prospectiva

Cuando hablamos acerca de algún *pronóstico*, significa que se ha establecido un enunciado claro sobre algo que es probable que suceda en el futuro, basándose en análisis y consideraciones de juicio. Medir esa probabilidad nos lleva directamente a consideraciones cuantitativas, que se consideran terreno propio de las matemáticas.

Al hacer un pronóstico, nuestra atención se centra en establecer lo que de alguna manera –totalmente determinística- se prevé que es lo más probable que llegue a suceder. Siendo esto una visión muy limitada de la construcción del futuro, pues no debemos limitarnos solamente a lo probable desdeñando lo deseable, lo posible, lo factible o lo que pueda representar un escenario totalmente adverso.

Hablar de pronóstico es plantearnos algo que puede darse en el futuro, pero no implica considerar todas las alternativas posibles de futuro con las que se pueda interactuar. Para ello, debemos referirnos a algo más amplio y diversificado; esto es, poder –en cierta forma– tratar de visualizar como dilucidar a través de una multiplicidad de escenarios de futuro, y desde esta óptica elegir el futuro más deseable y a la vez factible, para tratar de proceder a participar de manera dinámica e interactiva en su diseño y construcción. A esto, es lo que llamamos asumir una actitud prospectiva hacia el futuro conceptualizándolo como devenir, o sea como un horizonte luminoso y atractivo, lleno de inmensas posibilidades.

Para referirnos a la prospectiva, podemos echar mano de algo que ha escrito al respecto Marco Carlos Ávalos R.¹¹

Estas son sus palabras:

“Prospectiva es una investigación rigurosa sobre el porvenir, en función del sistema socioeconómico en su conjunto, y que puede aprehenderse en función de las grandes tendencias históricas de evolución de ese sistema. La prospectiva no es utopía. La prospectiva no es previsión.

La prospectiva no tiene la pretensión de predecir, sino de reflexionar sobre fenómenos que sucederán. La prospectiva puede prepararnos para todo tipo de acontecimientos. Se dice: si esto puede continuar así, puede producirse esto o lo otro. La prospectiva nos prepara para reaccionar ante diversas circunstancias, de las cuales se producirá una sola. La prospectiva imagina varios futuros, situaciones que pueden suceder y lo que se debería hacer según el caso.

Hay muchas definiciones de Prospectiva, pero en términos generales, la prospectiva es: Hacer probable el futuro más deseable.

Actitud de la Mente Hacia la Problemática del Porvenir.

La trayectoria de la prospectiva viene del futuro al presente. Es decir viene del porvenir al presente. La prospectiva es primero un acto imaginativo y de creación; luego una toma de conciencia y una reflexión sobre el contexto actual; y por último, un proceso de articulación y

¹¹ Ávalos R., Marco Carlos. “¿Qué es la Prospectiva?”.

<http://marcocar.tripod.com/>

(Consultado el lunes 16 de abril de 2012).

convergencia de las expectativas, deseos, intereses y capacidad de la sociedad para alcanzar ese porvenir que se considera deseable.

*La Prospectiva tiene un carácter creativo, es un elemento de cambio y transformación para asumir una actitud activa hacia el mañana, a través de la construcción y elección de “futurables” (futuro deseable) y futuribles (futuro posible)”.*¹²

1.2.2.- Métodos y técnicas de pronóstico para intentar visualizar futuros.

Tal como se especificó en la sección anterior, las técnicas de pronóstico constituyen una base importante para la prospectiva, en lo que concierne al análisis preliminar de futuros probables. Abajo, tratamos de establecer un cuadro que especifica las principales técnicas que se utilizan en toda la orbe.

CUADRO CONCERNIENTE A ALGUNAS TÉCNICAS DE PRONÓSTICO¹³

Técnicas de juicio o cualitativas

Características	Horizonte	Descripción
Funcionan cuando hay falta o escasez de datos históricos y cuando es difícil convertir en números las variables que intervienen en la determinación de la demanda	Normalmente se utilizan para planear a mediano y largo plazos.	<p>1. Opiniones de los gerentes/ejecutivos: se basa en la opinión general de un grupo de directivos o gerentes de la empresa.</p> <p>2. Técnica Delphi: un grupo de expertos responde, de manera anónima, a un cuestionario que pregunta sobre las proyecciones de ventas de la empresa. Un</p>

¹² Quizá, tratando de ser más rigurosos en el uso del lenguaje, podríamos sustituir –cuidadosamente- la palabra “porvenir”, de la cual el autor podría estar haciendo uso y un poco de abuso, por la palabra “devenir” que es más propia de la escuela voluntarista de la Prospectiva. Pero debemos de ser muy precisos al redactar, para no alterar el significado que el autor quiere en realidad expresar.

Tal pareciera que la palabra “porvenir” da más pie a la *utopía por la utopía misma*, que *al futuro cómo algo que se construye*, la palabra “devenir” es más propia para algo que *acaece y es capaz de transformarse*.

¹³ Las técnicas elegidas, corresponden a las mencionadas por Jorge Durán en su artículo publicado en agosto de 2005 en la página de **EntrepreneurEnEspañol.com**:

“15 técnicas de pronóstico”.

<http://www.entrepreneurespanol.com/pagina.hts?N=14912>

(Consultado el miércoles 25 de junio de 2008).

futura. La mayoría es de bajo costo y no requieren –a priori- de equipo computacional – sofisticado- para hacerse, aunque su planeación implica una gran inversión de tiempo por parte de los directivos.

moderador lee en voz alta las respuestas y, entre todos, buscan consenso.

3. Información de los vendedores: consiste en recopilar las estimaciones realizadas por los vendedores (o distribuidores) acerca de las ventas esperadas en sus territorios, con el fin de suponer la tendencia y cambios futuros.

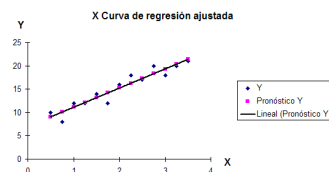
4. Análisis del ciclo de vida: se basa en la evaluación de las etapas de un producto o servicio para predecir su demanda en el mercado. Esto es, desde la introducción, inicio y crecimiento, hasta las etapas de madurez y declinación.

5. Investigación de mercados: se propone recolectar datos de diversas maneras (entrevistas, cuestionarios) para probar hipótesis acerca del mercado.

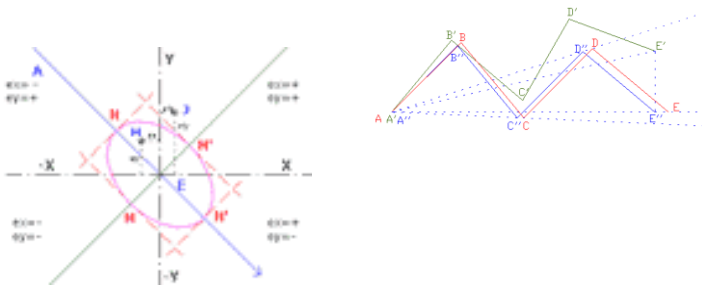
TÉCNICAS CUANTITATIVAS

Técnicas causales

Características	Horizonte	Descripción
Relacionan variables internas o externas con los niveles de demanda, lo que brinda una visión amplia del sector. Los costos que implican son de medios a bajos y usualmente requieren de equipo de cómputo.	Son más útiles para elaborar pronósticos a mediano plazo de productos o servicios existentes y para el diseño de estrategias de marketing, producción y contratación de personal.	Regresión: se predice la demanda futura a partir de una línea recta –o de otro tipo- formada por los datos de demandas pasadas. Si sólo se usa una variable del pasado se le llama regresión simple. Si se usan dos o más variables del pasado, se le nombra regresión múltiple.



Simulación: se trata de modelos dinámicos, usualmente basados en computadoras, que cruzan los datos de las variables internas (capacidad de producción, por ejemplo) y externas (niveles de poder adquisitivo de su mercado) para pronosticar la demanda.



Técnicas de series de tiempo

Características

Establecen relaciones entre el tiempo y los niveles de demanda. Su costo tiende a ser bajo, excepto para algunas técnicas como Box-Jenkins, que implica un software un tanto oneroso.

Horizonte

Se utilizan para el corto y mediano plazos y se aplican al manejo de inventarios, control de precios, programas de promociones y para considerar movimientos estacionales o cíclicos de la demanda. Requieren el uso de equipo y paquetes de cómputo.

Descripción

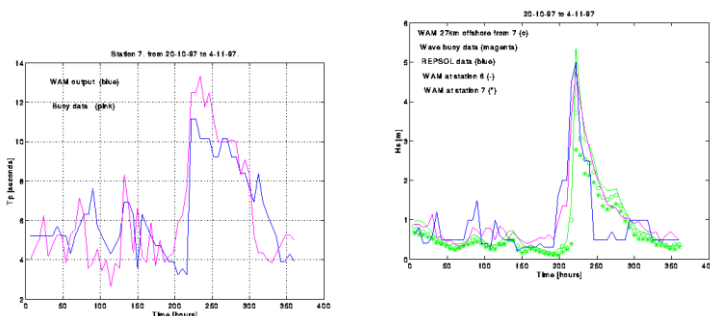
Proyección de Línea Recta: predice la demanda a partir de una línea recta en la que se han incluido los datos de demanda a través del tiempo.

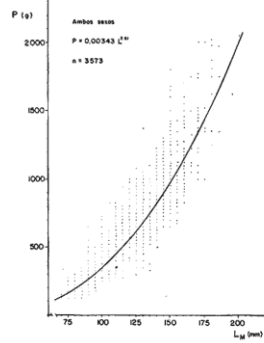
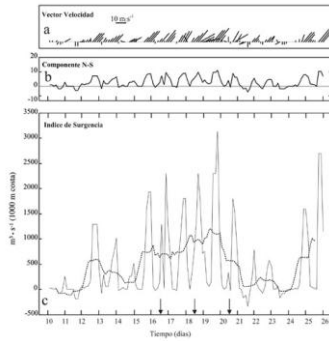
Promedios móviles: promedia los valores de demanda reciente para predecir la demanda futura.

Naive: es la aplicación de un supuesto simple: en el próximo periodo se repetirá la demanda actual.

Suavización exponencial: consiste en estimar la demanda del próximo periodo basándose en una combinación de indicadores de la demanda reciente y de los pronósticos pasados.

Descomposición clásica: es la predicción de la demanda esperada a partir de la tendencia, estacionalidad y “ciclicidad” que se han registrado en el pasado (en los





dos últimos años, por ejemplo).

Box-Jenkins: cruza varias series de tiempo para obtener otra serie de tiempo (o más de una) que permita estimar la demanda futura.

Combinaciones de cualitativas y cuantitativas

Sistemas expertos: consiste en la combinación de juicios cualitativos y métodos cuantitativos. Es decir, a partir del conocimiento empírico del negocio se busca el sustento de la información mediante la aplicación de una o varias técnicas cuantitativas de pronósticos.

Redes Neuronales: técnica adaptativa --"que aprende o se adapta"-- y automatizada. Es capaz de procesar varias series de datos y cruzarlas entre sí. Puede manejar discontinuidades (saltos abruptos) en la información. Su desarrollo requiere equipo de cómputo.

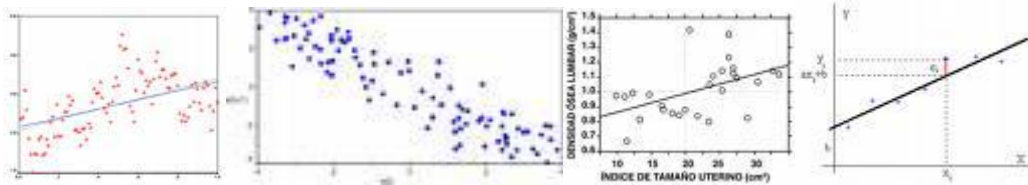
1.2.3.- PRECISIONES SOBRE ALGUNOS MÉTODOS¹⁴

Mínimos cuadrados: “Es una técnica de optimización matemática que, dada una serie de mediciones, intenta encontrar una función que se aproxime a los datos (un “mejor ajuste”).

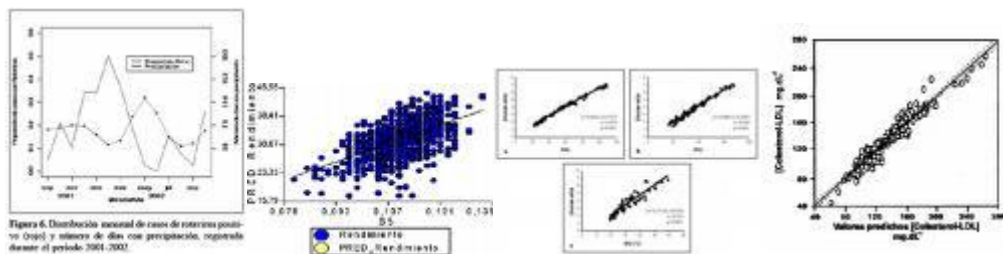
¹⁴ Para un mejor entendimiento de los conceptos vertidos en esta sección se recomienda la lectura de: “**LAS MATEMÁTICAS EN LAS CIENCIAS SOCIALES**”. Daniel Peña Sánchez de Rivera. Encuentros multidisciplinares, ISSN 1139-9325, Vol. 8, Nº 23, 2006 (Ejemplar dedicado a: matemáticas interdisciplinares en el siglo XXI). Págs. 67-79.

<http://dialnet.unirioja.es/servlet/articulo?codigo=2010248&orden=136534&info=link>
(Consultado el miércoles 25 de junio de 2008),

Intenta minimizar la suma de cuadrados de las diferencias ordenadas (llamadas *residuos*) entre los puntos generados por la función y los correspondientes en los datos”.¹⁵



Análisis de regresión: Es la parte de la estadística que se ocupa de estudiar cómo una variable se relaciona con otras variables de tipo cuantitativo. Por ejemplo, en estos tiempos en que el precio del crudo al parecer seguirá subiendo su costo, sería interesante a partir de una serie diaria de precios durante lo que va del sexenio, determinar una ley matemática que relacione a éste con el tiempo (o incluso agregar otras variables como el comportamiento del dólar, del euro y de las tasas de interés bancarias) No necesariamente tiene que tratarse de algo preciso, pero sí que se ajuste a un mínimo de error o incertidumbre.



En este tenor de las cosas, tratar de ir más al detalle en conceptos tales como promedios móviles, series de tiempo, técnicas de Box y Jenkins, etc., requiere de una adecuada formación técnica, para entender realmente lo que se está haciendo (y su sentido en la prospectiva estratégica). El lector interesado puede darse una idea de ello, emprendiendo un estudio concienzudo del análisis de impacto de tendencias¹⁶.

¹⁵ WIKIPEDIA. La enciclopedia libre. “**Mínimos cuadrados**”.

http://es.wikipedia.org/wiki/M%C3%ADnimos_cuadrados

(Consultado el lunes 16 de abril de 2012),

¹⁶ Jay Gordon, Theodore. “**TREND IMPACT ANALYSIS**”. The Milenium Proyect- Research Futures Methodology – V.3.0.

<http://test.scripts.psu.edu/students/d/j/djz5014/nc2if/08-Trend%20Impact%20Analysis.pdf>

(Consultado el lunes 16 de abril de 2012).

II.- VIRUS Y ANTIVIRUS

“Miro a mi alrededor veo que la tecnología ha sobrepasado nuestra humanidad, espero que algún día nuestra humanidad sobrepase la tecnología”. Albert Einstein.

“Sin duda ha habido muchas teorías con respecto al inicio de la corriente vírica, una de ellas apunta a que fueron las casas fabricantes de software para evitar la copia ilegal de sus programas. Sin embargo esto no tiene mucho sentido, ya que esas mismas casas tendrían que reponer miles de copias de sus productos y estarían de esta forma tirando piedras contra su propio tejado”. Luis de la Iglesia Rodríguez.

Los virus informáticos y las diversas variantes de código malicioso (llamado también *malware* o código malicioso) pueden ser temibles para usuarios que nunca los hayan encontrado antes. Estos a veces reaccionan con pánico o de manera impulsiva ocasionando más problemas que soluciones, pues los virus no afectan solamente a la información de las computadoras, afectan a los usuarios, la presencia de un virus en la computadora provoca un daño a su propietario. Puede ser perjuicio económico o acentuado “estrés”, y hasta crisis nerviosas cuando ocurren pérdidas que se presumen irreparables.

La noción usual (digamos clásica) de virus informático fue establecida en el año 1984, durante la conferencia IFIC/SEC´84 por el Doctor Fred Cohen quien lo definió como un “software maligno capaz de reproducirse a sí mismo” y estableció paralelismos entre los virus biológicos y los informáticos para justificar la adopción de dicha terminología. Con la palabra *malware* definimos todo código cuyo fin es llevar a cabo acciones nocivas contra un sistema informático.

Existen actualmente diversas variantes de código malicioso. A saber:

- a). – Los virus (en el sentido estricto del término), que para reproducirse utilizan archivos a los cuales inoculan su código.
- b). – Los gusanos, los cuales generan copias de sí mismos y viajan a través de una red, o incluso a través de Internet.
- c).- Las bombas lógicas, que son pequeños programas camuflados dentro de otros y se activan de acuerdo a determinadas circunstancias como pueden ser una fecha, una combinación de teclas o algún tipo de contador.
- e).- Programas que capturan lo que se escribe en el teclado, llamados keyloggers.

f).- Puertas traseras, que permiten operar el equipo de cómputo de manera remota, como si literalmente estuviéramos sentados frente a él. Esto incluye tomar posesión –incluso- de una red –o hacer que el equipo o equipos (lo que se suele llamar *botnets*), se usen para atacar cuentas bancarias o romper gradualmente candados de servidores, sin excluir ataques de negación de servicio.

d). – Los Caballos de Troya (o Troyanos), los cuales son programas de apariencia completamente normal pero que en realidad incorporan código que puede dañar a una computadora, instalar una puerta trasera (acceso ilegítimo o no autorizado) o cualquier otra acción perjudicial para el usuario.

Dada esta diversificación –que año con año se vuelve más amplia, rebasando lo contenido en los glosarios que sobre el tema se vayan generando-, es como los antivirus ya no solamente se ocupan de los virus sino que se orientan a prevenir todas estas variantes de código malicioso y ataques de aplicaciones potencialmente dañinas. Curiosamente les seguimos llamando antivirus y no “*antimalware*”, aunque sería más lógico actualizar la noción de virus y en los tiempos actuales no considerar “un abuso de lenguaje” utilizarla como sinónimo de malware. De hecho, en el escenario actual las amenazas son mayormente los gusanos y los troyanos seguidos de los virus y las bombas lógicas, y otra serie de “linduras” que derivan de ellas.

Todo lo anterior fue necesario precisarlo, pues los virus tan temibles a los que se suelen referir los medios en el advenimiento del siglo XXI, constituyen en realidad la familia de gusanos (y troyanos) del nuevo milenio. De esta manera la responsabilidad del usuario ya no se limita solamente a mantener su antivirus actualizado y bien configurado, sino que se requiere mantener al día la instalación de los distintos parches de Seguridad de Microsoft, pues los gusanos y troyanos suelen explotar las vulnerabilidades que éstos permiten cerrar, apostando más al empleo de verdaderas suites de seguridad, que integran antivirus, antispyware, firewall y herramientas adicionales.

Es recomendable recurrir la consulta directa de las enciclopedias de virus que pueden hallarse en las páginas electrónicas de las distintas empresas de antivirus y estar pendiente de las alertas que emitan. Del mismo modo, no debemos hacer caso a los mensajes que se reciben por correo haciendo alusión a virus catastróficos y apoyándose en que tal o cual firma

antivirus lo dice, sin antes cotejar las fuentes directamente, siempre es mejor suscribirse a los boletines de información de las empresas y así mantenerse bien informado.

II.1.- LA GÉNESIS Y EL DEVENIR DE LOS VIRUS INFORMÁTICOS

"Supóngase que existe un algoritmo general A que, analizando cualquier programa P, devuelve "verdadero" si y sólo si P es un virus. Entonces sería posible crear un programa P, que hiciera lo siguiente: sí (A (P) = falso) entonces infecta el sistema, si (A (P) = verdadero) implica no infectes nada. Es decir, P es un virus si A dice que no lo es, y no lo es si A dice que lo es. Por contradicción, ese algoritmo general A no existe."

"Se le llama Virus Informático a todo programa capaz de infectar otros programas, modificándolos para incluirse dentro de los mismos"

Estas dos afirmaciones corresponden a una parte del trabajo titulado *"Virus Informáticos: teoría y experimentos"*¹⁷, cuyo autor es el Doctor Fred Cohen quien es reconocido como *el primero en definir los virus informáticos*, lo cual tuvo lugar durante un discurso en la Universidad de California, en el año de 1984. En su intervención incluyó los ejemplos para el desarrollo de estos programas "auto replicables" y donde además de dar una definición los tilda como el mayor y más grave problema para la seguridad nacional y el futuro de la informática.

De hecho esta historia se remonta al 3 de noviembre de 1983, que fue cuando *el primer virus fue concebido* como un experimento para ser presentado en *un seminario semanal de Seguridad Informática*. El concepto fue introducido por el propio Cohen y el nombre virus fue dado por Len Adleman. Tuvieron que pasar ocho horas de trabajo en una VAX 11/750 ejecutando UNIX, para que este primer virus quedara listo para su demostración. Finalmente fue hasta el 10 de noviembre de ese año, en que después de obtener las autorizaciones necesarias y concluir cinco experimentos el virus fue mostrado.

Una de las principales contribuciones que se dieron en este trabajo fue la de *esclarecer que ningún detector de virus puede ser perfecto*, en el sentido que nos permita un mecanismo de verificación inequívoco al 100% para decidir si un programa dado reúne o no las condiciones

¹⁷ Cohen, Fred & Associates (Specializing in Information Protection Since 1977). "Computer Viruses – Theory and Experiments." Copyright ©, 1984. URL: <http://all.net/books/virus/index.html> (Consultado el lunes 16 de abril de 2012).

para considerarlo como un virus. En otras palabras, no es factible tener un algoritmo universal que nos permita arreglárnoslas de una vez por todas y para siempre con estos “*bichitos*”.

Es de esta manera como se explica esa *lucha sin fin entre los virus y los antivirus*, cuyas pautas vienen marcadas por las tendencias en la evolución misma de la tecnología y su impacto sobre las modalidades que se van dando en la creación de los códigos maliciosos. No obstante, gracias a que existe un sustento bastante sólido para este tema, es como hoy en día es factible la creación casi inmediata de soluciones a los distintos virus nuevos que se van presentando.

Hasta los años ochenta, el término virus (del latín veneno) solamente se empleaba dentro del ámbito de las ciencias médicas y biológicas para definir a microorganismos capaces de penetrar en el ser humano y destruir o alterar el contenido genético celular provocando diversos cuadros patológicos. Precisamente por ciertas semejanzas con su modo de actuar y las características de sus efectos, fue como a ciertos programas que pueden auto-reproducirse (“transmitirse” de una computadora a otra, pudiendo causar daños a la información y al sistema mismo) se *les bautizó como virus informáticos*.

En realidad el origen de estos no es algo tan simple de precisar. Aunque los más diversos especialistas convienen en señalar que fue John von Neumann en su artículo “*Theory and Organization of Complicated Automata*” quien estableció por vez primera la idea de una porción de código capaz de reproducirse a sí mismo.

Hasta hace pocos años, la mayoría de los virus solían programarse solamente en lenguaje ensamblador, por sus posibilidades y el nivel de optimización que permite, pero con el innegable avance de los sistemas operativos de 32 y 64 bits, el Internet y el correo electrónico, la combinación del lenguaje ensamblador con lenguajes de alto nivel es una idea cada vez más empleada. Lo anterior, dado que la tendencia natural es la de *encaminar el mundo de los virus hacia el hacking, haciendo posible que los virus puedan robar los archivos de contraseñas de una computadora y conseguir su ilegítimo envío a una cuenta de correo establecida de antemano*, poniendo de manifiesto la extrema inseguridad de los sistemas operativos actuales.

En el fondo, la inexistencia de un algoritmo universal para replicar y anular cualquier virus posible, depende de la imposibilidad de poder crear un algoritmo que permita “dadas dos

proposiciones arbitrarias de contenidos también arbitrarios, decidir si tienen alguna relación lógica o cuantitativa”.

II.2.- PANORAMA ACTUAL DE LOS DISTINTOS ANTIVIRUS

“Es mejor saber después de haber pensado y discutido que aceptar los saberes que nadie discute para no tener que pensar.” Fernando Savater.

"Saber no es suficiente, debemos aplicar. Desear no es suficiente, debemos hacer."

Johann W. von Goethe."

"La clave está en las actualizaciones: un antivirus sin soporte no sirve más que un reloj sin manecillas (o sin baterías si es electrónico)." José Anaya

En la actualidad, es claro muchas personas están conscientes de la necesidad de hacer uso de algún antivirus o “*suite*” de seguridad, como medida de protección básica para sus equipos de cómputo. No obstante, en principio lo deseable sería poder tener un panorama de los distintos productos que existen y con ello, una guía inicial para proceder a evaluarlos. El objetivo de este capítulo, es facilitar -en primera instancia- dicha tarea. Nos ocuparemos solamente de algunos de estos productos, enlistando la empresa con la dirección de su página de internet, añadiendo información escueta proporcionada por su *CEO*, *partner* o *reseller*.

- AhnLab - Antivirus Software and Security Solutions Provider.
(<http://global.ahnlab.com/en/site/main/main.do>).
- Antivirus Commtouch - Internet Security Solutions.
(<http://www.commtouch.com/antivirus>).
- Antivirus Download, Antivirus-Software, Bankguard, Mobile Security - G Data Software AG. (<http://www.gdata.de/>)
- Anti-Virus Leader ViRobot. (<http://www.hauri.net/>).
- Antivirus Software - Bitdefender Security Solutions. (<http://www.bitdefender.com/>).
- Antivirus Software Symantec. (<http://www.symantec.com/endpoint-protection>).
- Antivirus, Endpoint, Disk Encryption, Email and Web Security Sophos.
(<http://www.sophos.com/en-us/>).
- Avast! : Free Antivirus o Internet Security. (<http://www.avast.com/es-mx/index>).

- Avira: seguridad para su PC bajo Windows y Unix. (<http://www.avira.com/es/index>).
- AVL MINI-Antiy Labs- Anti-Virus-Anti-Trojan. (<http://www.antiy.net/product/avl/>).
- Best internet security Top antivirus protection Laptop tracking Anti spam software. (<http://www.quickheal.co.in/>).
- ByteHero Information Security Lab
<http://www.bytehero.com/english.asp>
- CA Technologies IT Management Software and Solutions. (<http://www.ca.com/us/default.aspx>).
- Central Command, Inc. Home. (<http://www.centralcommand.com/>).
- Clam AntiVirus. (<http://www.clamav.net/lang/en/>).
- AVG Free Anti-Virus. (<http://www.freeavg.com/?lng=mx-es&cmpid=corp>)
- Dr. WEB. (<http://www.drweb.com/>).
- Endpoint Protection, Antivirus Software, Email & Anti-Malware Protection - GFI Software. (<http://www.sunbeltsoftware.com/>).
- eSafe Content Security Solutions for Web and Mail Gateways. (<http://www.safenet-inc.com/data-protection/content-security-esafe/>).
- ESET - Antivirus Software with Spyware and Malware Protection. (<http://www.eset.com/us/>).
- Fortinet (<http://www.fortinet.com/>).
- F-PROT Antivirus. (<http://www.f-prot.com/>).
- F-Secure. (http://www.f-secure.com/en/web/home_global/home).
- Emsisoft Anti-Malware (<http://www.emsisoft.mx/es/>).
- McAfee-Antivirus (<http://www.mcafee.com/mx/>).
- Panda Security (<http://www.pandasecurity.com/mexico/>).
- IKARUS Security Software GmbH Antivirus program - virus scanner - virus protection. (<http://www.ikarus.at/en/>).
- VirusBuster Antivirus & Antispam. (<http://www.virusbuster.hu/>).
- Kaspersky Lab. (<http://latam.kaspersky.com/?sitepref=mexico?>).
- Microsoft Malware Protection Center. (<http://www.microsoft.com/security/portal/>).
- Norman — Proactive IT security. (<http://www.norman.com/>).
- nProtect GGP 3.0.

(http://global.nprotect.com/GGP_download/index.php?user_lang=en).

- Online Defence System for Home & Enterprise - K7 Computing.
(<http://www.k7computing.com/en/>).
- PC Tools Antivirus Software & PC Software Utilities. (<http://www.pctools.com/>).
- Trend Micro. (<http://la.trendmicro.com/la/home/>).
- Comodo Creating Trust Online. (<http://www.comodo.com/>).
- SUPERAntiSpyware. (<http://www.superantispyware.com/>).
- Virus Block Ada (VBA) 32 Antivirus. (<http://www.anti-virus.by/>).
- Rising Lion – Strong Security. (<http://www.rising.com.cn/>).

Esta sin duda no es una lista completa y difícilmente podría serlo. Corresponde exclusivamente al grupo de antivirus con los cuales he tenido cierta experiencia en los últimos años y por ende recomiendo por lo menos una vez en la vida tomarse la molestia de conocerlos y evaluarlos. Todo esto en la medida de que el interés por el tema sea lo suficientemente grande.

Tratando de ir a lo fundamental, se tienen comúnmente dos distintos enfoques:

1. El del administrador de una empresa corporativa que desea prioritariamente tener resuelto el problema de administración centralizada. Es decir desea de un antivirus que posea una consola que permita la instalación remota tanto en una red LAN como en una WAN y no verse obligado a instalar el producto a pie en cada una de las estaciones de trabajo. La experiencia ha demostrado que por lo regular cuando esto se logra no siempre hay la garantía de que la calidad en la detección y la limpieza sea de lo mejor. (Además, en muchas ocasiones se han descubierto vulnerabilidades como costo natural por tantas bondades de las “consolas que suelen lanzar fuegos artificiales”, la comodidad excesiva para los administradores de una red no siempre garantiza que la seguridad no sea comprometida).
2. El del usuario final al cual lo que le interesa es no infectarse por ningún motivo y que la protección en memoria del producto sea de lo más eficaz, tanto para detectar y remover cualquier virus que pueda presentarse. Pero cuando esto se da, también suele suceder que las prestaciones de dicho antivirus para administrarlo llegan a ser muy limitadas.

Tal parece que lo ideal para una empresa es tener bien estructurado un equipo de personas que procuren entender responsablemente ambos enfoques.

Ningún producto en el mercado puede garantizar que se tendrán eficientemente el total de todas las prestaciones deseables. Por ello, más que procurarse el mejor antivirus o suite de productos de seguridad (incluyendo los criptográficos), lo que se necesita es diseñar las mejores estrategias de seguridad acordes a la problemática que se tenga. A veces no basta con una sola elección.

En virtud de lo anterior, al hacer una evaluación es importante tratar de verificar hasta que punto los diversos antivirus –*antimalware*– que vayamos a considerar cumplen con las siguientes características:

- I. Deben actualizar los patrones o firmas en pocas horas, además poseer un buen motor heurístico.
- II. La empresa que los promueve debe contar con un equipo de soporte técnico con acceso a un laboratorio especializado en códigos maliciosos y un tiempo de respuesta no mayor a 24 horas, el cual pueda orientar al usuario en su idioma, en caso de que contraiga una infección o tenga dificultades con el producto.
- III. Deben contar con distintos métodos de verificación y análisis de posibles códigos maliciosos, incluyendo el heurístico, el cual *no se basa en firmas vírales sino en el comportamiento de un archivo*. Y así poder detener amenazas, incluso de posibles *virus nuevos*.
- IV. Deben poderse adaptar a las necesidades de diferentes usuarios.
- V. Deben poder realizar la instalación remota tanto en una red LAN como en una WAN.
- VI. Deben constar de alguna consola central en donde se puedan recibir reportes de virus, mandar actualizaciones y personalizar a distintos usuarios. Todo esto, siempre y cuando se garantice que no se compromete de manera alguna la seguridad debido a vulnerabilidades no contempladas.
- VII. Deben ser verdaderamente efectivos para efectos de detección y eliminación correcta y exacta de los distintos virus que puedan amenazar a los sistemas.
- VIII. Deben de permitir la creación de discos de emergencia (CD, DVD) o de rescate de una manera clara y satisfactoria.
- IX. No deben de afectar el rendimiento o desempeño normal de los equipos. De ser preferible lo que se desea es que su residente en memoria sea de lo más pequeño. También se espera que su motor de búsqueda sea rápido y eficiente.

X. El número de falsos positivos que se den tanto en el rastreo normal como en el heurístico debe de ser el mínimo posible. La empresa debe de corregir en poco tiempo los "bugs" y los falsos positivos que se le reporten.

XI. Su mecanismo de auto-protección debe de poder alertar sobre una posible infección a través de las distintas vías de entrada, ya sea Internet, correo electrónico, red, USB, etc.

XII. Deben de tener posibilidad de inspeccionar el arranque, así como los posibles cambios en el registro de las aplicaciones, y responder activamente en caso de enfrentarse a páginas contaminadas (deteniendo cualquier tipo de intrusión).

Con todas estas pautas anteriores, consideramos que se pueden tener los elementos suficientes que nos permitan ponerlos a prueba y de acuerdo con nuestras prioridades poder establecer nuestras propias conclusiones.

UN PUNTO DE VISTA PERSONAL:

1).- El enfoque de crítica a las certificaciones no es preciso del todo. Pues *Virus Bulletin*, *ICSA Labs*, se aplican de manera muy explícita a los especímenes que pueden ser considerados como virus en todo el sentido de la palabra y cuya peligrosidad ya sea grande o relativa no está puesta a duda, no se enfocan tan fuertemente al problema de gusanos, troyanos, backdoors, –a menos que su difusión constituya en el mundo una amenaza clara-; y demás variantes de malware (código malicioso), pues este no es su objetivo ni tampoco es sencillo agotar el tema. *Los antivirus no son un software "anti-lo-que-sea"*.

2).- Con las certificaciones más comunes, se ha analizado la eficacia relativa sin llegar al fondo de la calidad relativa de la limpieza de cada producto y por lo regular no suelen enfocarse por igual a arrojar análisis en todas y en cada una de las plataformas, como sería lo deseable.

3).- Irnos por el lado de ISO (certificación de calidad total), nos daría garantía de que como empresa certifican que tienen cierta calidad en sus procesos y los documentan. Esto es más bien garantía de seriedad y cumplimiento de estándares comúnmente aceptados, pero esto por sí solo no acredita holgadamente la eficacia ni la eficiencia. El caso de los antivirus, tanto como producto así como servicio suele ser más delicado. Una empresa antivirus que tenga ISO, no por ello ya "la hizo".

4).- Más que las certificaciones y las comparativas, lo ideal sería poder evaluar y comparar la velocidad real de los laboratorios de las empresas antivirus ante una amenaza real, cómo responden, a qué velocidad y que tan sólida o buena suele ser su respuesta.

5).- Actualmente no existen comparativas serias para evaluar la capacidad heurística, pues existe una profunda controversia sobre el tema.

Quedan abiertas –como una invitación a la reflexión- algunas preguntas a las cuales se les da una respuesta inicial o tentativa (que en su momento fueron discutidas a fondo con José Anaya Pedrero de CIBERSEL):

1).- ¿Es o no importante que alguien pueda finalmente certificar la calidad de respuesta de los laboratorios de las empresas antivirus ante una nueva amenaza?

- Desde luego que no solo es importante, sino crucial. Eso pondría a cada quien en su lugar. Porque de esa manera, los antivirus con una buena heurística quedarían muy por encima de otros que sin definiciones dejan pasar todos los nuevos virus en las primeras horas de difusión.

2).- ¿Es importante o no que alguien pueda certificar que las bases de los antivirus no incluyan a virus que no son tales?

- Solo por razones de eficiencia, no de eficacia. Se puede vivir con eso mientras no repercuta sensiblemente en el desempeño del sistema, pues con los virus que hay ya es suficiente. Este problema va de la mano de la pregunta anterior, los antivirus con buena heurística no se ven afectados por una base de datos inflada artificialmente, porque solo recurren a ella cuando ya se confirmó la presencia de un intruso. En cambio los antivirus que están atados a la base de datos, como sucede con algunos de los más comerciales, sí llegan a impactar el desempeño. Hay que reconocer que de todos modos, estos no siempre tienen la reputación de inflar sus bases de datos.

3).- ¿Qué aspectos en los antivirus son importantes y hasta la fecha nadie los contempla en las certificaciones?

- La velocidad de respuesta ante un nuevo espécimen que les es enviado para análisis. También la capacidad de reacción ante nuevas tecnologías virales que no pueden atacarse con solo la actualización de definiciones. De nuevo, este es un talón de Aquiles de ciertos antivirus apoyados bastante por el "marketing", pues el usuario tiene que esperar hasta que

sale la nueva versión del programa o conformarse con una solución ad-hoc que es inadmisibile en el contexto corporativo, donde no se puede pretender que se descontaminen a mano 3,000 o más equipos. La capacidad de actualizar componentes y no solo definiciones, a menudo no es ponderada con la seriedad debida y puede más una marca o un anuncio que los méritos tecnológicos del producto. Esto se debe en buena parte a que los evaluadores corporativos aplican los mismos parámetros para seleccionar la suite de Office que un antivirus

III.- CIBERCRIMEN

“Así que no lo temáis, porque nada hay encubierto que no haya de ser descubierto, ni oculto que no haya de saberse.” Jesús de Nazareth (Mateo 10:26).

“La información quiere ser libre”. *Mantra original de los hackers.*

“Los países más desarrollados son en realidad los más vulnerables a la guerra cibernética y el ciberterrorismo, y la única manera de mitigar esta amenaza es a través de la cooperación internacional. La guerra cibernética ha sido una de las mayores preocupaciones de los profesionales de la seguridad en tecnologías de la información en los últimos años.” Eugene Kaspersky.

Una primera aproximación al tema, necesariamente conlleva a procurar precisar varios conceptos. La primera sutil filigrana que hay que desentrañar, es la frontera entre los términos cibercrimen -o ciberdelito- y ciberterrorismo, así como el mito y realidad de ambos conceptos como una posible y –a la vez- dramática realidad actual. (Un acto terrorista es un delito porque infringe a la Ley, pero los actos delictivos no necesariamente son terroristas).

Preliminarmente, establecemos como bases de reflexión, algunas versiones aproximadas de lo que dimensionamos como terrorismo –*cuando lo impensable sucede*-, las puntualizamos de manera gradual:

- “Uso de la intimidación coercitiva por los movimientos revolucionarios, regímenes o individuos, por motivos políticos.”¹⁸ (Lo que suele suceder en buena medida, pero sin saber exactamente a lo que nos estamos enfrentando).

¹⁸ Wilkinson, Paul: *Political Terrorism*, Macmillan, Londres, 1974, pp. 11-12.

- Definición oficial del FBI: “Uso ilegal de la fuerza o la violencia contra personas o propiedades a fin de intimidar o cohercionar al gobierno, la población civil o cualquier otro segmento, persiguiendo objetivos sociales o políticos.” (Noción que se estrella ante el crisol de las guerras de liberación de los pueblos y sus motivos de justificación de la defensa, yendo más allá del concepto del Estado como único actor político que posee el monopolio del uso de la violencia legítima como salvaguardia del orden social e institucional. ¿Bajo qué parámetros podemos discernir entre el ataque de un terrorista o alguien que lucha por la libertad?).

Jessica Stern nos da bastante luz sobre el tema. Explícitamente nos dice:

”La literatura nos ofrece cientos de definiciones del terrorismo. Algunas ponen acento en los terroristas; otras, en los fines que éstos persiguen, y otras en las técnicas empleadas. Sin embargo, sólo dos son las características esenciales que distinguen al terrorismo de otras formas de violencia. En primer lugar, el terrorismo se dirige contra personas que no tienen la calidad de combatientes, diferenciándose así de la guerra. Y en segundo lugar, los terroristas emplean la violencia con una finalidad bien precisa, que por lo general es la de infundir miedo al grupo elegido como blanco de sus ataques. Esta provocación deliberada del miedo es lo que separa al terrorismo del simple asesinato o agresión violenta.

Definimos entonces el terrorismo como empleo o amenaza de violencia contra no combatientes, con una finalidad de venganza o intimidación, o para influir de alguna otra forma sobre un determinado sector de la población. Con esta definición se evita limitar demasiado el círculo de los perpetradores o sus propósitos, admitiendo una gama amplia de posibles actores (que incluye a los Estados y sus agentes, grupos internacionales o individuos aislados) y motivos aparentes (políticos, religiosos o económicos), además del asesinato por el simple gusto de matar.”¹⁹

Consecuentemente –no haciéndose necesario un debate sobre lo que es Internet y los delitos informáticos- podemos aventurarnos a explicitar -al sugerir la palabra *ciberterrorismo* un lugar común entre *ciberespacio* y terrorismo-, que estamos hablando del ataque premeditado y políticamente motivado contra información, sistemas computacionales, programas de

¹⁹ Stern, Jessica (2001): “**EL TERRORISMO DEFINITIVO**” Ediciones Granica, S.A. ISBN: 84-7577-899-2. Impreso en España publicada por acuerdo del editor original. Pág. 33.

computadoras y datos que puedan deliberar en violencia contra objetivos por parte de grupos *subnacionales* o agentes clandestinos.

No todo aquello que pueda considerarse un delito en Internet, necesariamente encaja en la noción de *ciberterrorismo* –terrorismo cibernético-, Dorothy E. Denning lo acota de la siguiente manera:

“Para calificar como ciberterrorismo, un ataque debe resultar en violencia contra personas o contra la propiedad, o al menos causar el daño suficiente como para generar miedo. Ataques que deriven en muertes o personas heridas, explosiones, colisiones de aviones, contaminación de agua o severas pérdidas económicas pueden ser ejemplos válidos. Serios ataques contra la infraestructura crítica de un país podrían ser actos de ciberterrorismo, dependiendo de su impacto. Los ataques que interrumpen servicios no esenciales o que son básicamente una molestia costosa no entran en esta categoría.”²⁰

Es menos complicado tipificar el cibercrimen que el ciberterrorismo –incluso no todo vandalismo cibernético o abuso, es necesariamente un delito susceptible de perseguirse– menos un acto terrorista. Señalamos –a continuación– una serie de prácticas que no necesariamente quedarían enmarcadas en el concepto de ciberterrorismo, aunque eventualmente puedan tratarse de cibercrimen:

- 1) El “*hackeo*” –o incursión ilegítima en su estructura– de sitios *web* y la modificación de sus contenidos.
- 2) Los ataques de negación de servicio (DOS), destinados a paralizar operaciones de un sitio.
- 3) Intromisiones no autorizadas en redes privadas o gubernamentales, aún tratándose de organismos vinculados a la seguridad estratégica de las naciones.
- 4) Espionaje industrial, robo de bases de datos, clonación de tarjetas de crédito, lavado de dinero a través de transferencias bancarias en cuentas digitales, y otras más que implican un beneficio económico o ataque a la integridad de la información de las instituciones, claramente son delitos cibernéticos – ciberdelitos o cibercrimen como sinónimo–.

²⁰. Denning, Dorothy E. (2000): **CYBERTERRORISM**. Special Oversight Panel on Terrorism, Committee on Armed Services. URL: <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html> (Consultado el viernes 27 de julio de 2012).

- 5) Diseminación de códigos maliciosos: virus, gusanos y otras “*ciberalimañas*”.
- 6) Saturación deliberada de casillas de correo electrónico (“*e-mail bombs*”).
- 7) Utilización de Internet por grupos terroristas con fines informativos y doctrinarios.
- 8) La desobediencia civil electrónica –“*hactivismo*”-, que no siempre configura escenarios de carácter delictivo, a menudo consiste solamente en trasladar las protestas de las calles a Internet, manifestada muchas veces a través de las redes sociales.

El cibercrimen es una amenaza que se manifiesta de manera frecuente, desde el momento en que es posible perpetrar delitos y consumarlos, utilizando las vías electrónicas y hasta satelitales. Lo que todavía tiene un aspecto más limitativo es el ciberterrorismo, pues no existe una abundancia bien documentada de casos de ocurrencia repetitiva o impredecible.

A MANERA DE CONCLUSIÓN

Termina aquí este libro, el primero que me atrevo a escribir en mi vida, dejando solamente como contribución las bases mínimas que al profundizarlas gradualmente nos permiten ubicarnos en la esencia de la inseguridad informática y el cibercrimen. Esto es, nada ni nadie está seguro, la seguridad informática es un sueño y a lo único que podemos realmente aspirar es a la disminución o prevención cada vez más eficaz de los riesgos, el mundo del cibercrimen se circunscribe a la apología del delito trasladada al ciberespacio.

Existen gran cantidad de trabajos destinados a presentar estadísticas minuciosas sobre las distintas modalidades de delitos cibernéticos. Es muy difícil discriminar cuáles son los que se asemejan más a una descripción clara, que nos permita -realmente- ser precisos en cuanto a la naturaleza, presencia y evolución de los distintos peligros en Internet que van surgiendo.

Mi objetivo nunca fue –al escribir estas líneas- lograr un tratado sobre la materia, sino sembrar en el lector la duda crítica sobre el tema. Hablar a profundidad sobre Inseguridad Informática y Cibercrimen, requiere de escribir minuciosamente sendas obras que nos lleven de la mano en materia de Virus Informáticos, Criptografía, y Detección de Intrusos, lo cual –en el futuro cercano podré cristalizarlo adecuadamente en tres libros escritos en el orden mencionado.

Ludwig Wittgenstein escribió alguna vez: *“Todo lo que ha de ser dicho, debe decirse con claridad. De las cosas que no se puede hablar es mejor callarse”*. En este tenor de las cosas, podemos asegurar que este libro fue escrito como la guía básica, que permite apreciar todo el caudal de conocimientos a los que se puede acceder consultando periódicamente las direcciones electrónicas:

<http://www.hispasec.com/>

<http://www.segu-info.com.ar/>

<http://www.inteco.es/>

<http://www.fbi.gov/>

<http://www.zma.com.ar/>

<http://www.seguridadydefensa.com.ar/>

En cada una de ellas se obtiene el conocimiento básico, para sensibilizarnos adecuadamente en la problemática.

REFERENCIAS:

- 1).- Ávalos R., Marco Carlos. **“¿Qué es la Prospectiva?”**. URL: <http://marcocar.tripod.com/> (Consultado el viernes 27 de julio de 2012).
- 2).- Berger Gastón. **“La actitud prospectiva.”** (2002). Dossier: Futuro y prospectiva. Revista Universidad de Guadalajara. Dirección electrónica:
http://mail.udgvirtual.udg.mx/biblioteca/bitstream/20050101/898/1/La_actitud_prospectiva.pdf
(Consultado el viernes 27 de julio de 2012).
- 3).- Cano, Jeimy José, Ph.D. (2008) **“Cibercrimen y ciberterrorismo. Dos amenazas emergentes.”** Artículo español, Journal Online. URL: <http://www.isaca.org/Journal/Past-Issues/2008/Volume-6/Documents/jpdf0806-cibercrimen.pdf> (Consultado el viernes 27 de julio de 2012).
- 4).- Cano, Jeimy José, Ph.D. (2004) **“Inseguridad informática: Un concepto dual en seguridad Informática.”** Universidad de los Andes, Facultad de Ingeniería. Revista de

- Ingeniería, No. 19, Mayo, 2004, pp. 40 - 44. ISSN 0121-4993 / E-ISSN 2011-0049. URL: <http://revistaing.uniandes.edu.co/pdf/Rev19-4.pdf> (Consultado el viernes 27 de julio de 2012).
- 5). - Cohen, Fred & Associates (Specializing in Information Protection Since 1977). **“Computer Viruses – Theory and Experiments.”** Copyright ©, 1984.
URL: <http://all.net/books/virus/index.html> (Consultado el viernes 27 de julio de 2012).
- 6).- Corren, Sean Paul y Corrons, Luis. **“El Negocio de los Falsos Antivirus, Análisis del Nuevo Estilo de Fraude Online.”** Panda Labs – Julio 2009. URL: <http://www.pandasecurity.com/img/enc/EI%20Negocio%20de%20los%20falsos%20antivirus.pdf> (Consultado el viernes 27 de julio de 2012).
- 7).- Cruz Moreno, Lic. Juan Carlos (2008). **”PROGRAMA PARA LA ASIGNATURA Prospectiva Estratégica.”** Facultad de Ciencias Políticas y Sociales (FCPyS) de la UNAM. URL: <http://pensarelfuturo.files.wordpress.com/2008/02/prospectiva-estrategica.pdf> (Consultado el viernes 27 de julio de 2012).
- 8).- Denning, Dorothy E. (2000): **CYBERTERRORISM**. Special Oversight Panel on Terrorism, Committee on Armed Services. Dirección electrónica: <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>
- 9).- Kaspersky Lab. **“Tu guía para frenar el Cibercrimen”**. URL: http://www.kaspersky.com/sp/images/tu_guia_para_frenar_el_cibercrimen.pdf
<http://catedradh.unesco.unam.mx/catedradh2007/SeguridadHumana/prospectiva%206/revista/numero%203/construf/conspira/wong.htm> (Consultado el viernes 27 de julio de 2012).
- 10).- Laboratorio de ESET Latinoamérica (17 de noviembre del 2011). **“Tendencias 2012, El malware a los móviles”**. Dirección electrónica: http://www.eset-la.com/pdf/prensa/informe/tendencias_2012_el_malware_a_los_moviles.pdf (Consultado el viernes 27 de julio de 2012).
- 11).- Laboratorio de ESET Latinoamérica (22 de noviembre del 2010). **“Tendencias 2011: las botnet y el malware dinámico”**. Dirección electrónica: http://www.eset-la.com/pdf/prensa/informe/tendencias_2011_las_botnet_y_el_malware_dinamico.pdf (Consultado el viernes 27 de julio de 2012).
- 12).- **“Larousse diccionario enciclopédico usual.”** Tercera edición (2007). Ediciones Larousse, S.A. de C.V., Londres núm. 247, México 06600, D. F.

- 13).- Miklos, Tomás y Tello, M^a. Elena. **“Planeación Prospectiva. Una estrategia para el diseño del futuro”**. Editorial Limusa, 2006. ISBN: 968 18388443. Dirección electrónica: <http://claroline.ucaribe.edu.mx/claroline/claroline/backends/download.php?url=L1BMQU5FQU NJT05fUFJPU1BFQ1RJVKFFTUITE9TX1fVEVMTE9fQ09NUExFVE8ucGRm&cidReset=true &cidReq=PROSPECTIVA> (Consultado el viernes 27 de julio de 2012).
- 14).- Panda Security, The Cloud Security Company. **“Informe Panda Security: El Mercado Negro del Cibercrimen al Descubierto”**. URL: <http://prensa.pandasecurity.com/wp-content/uploads/2011/01/Mercado-Negro-del-Cybercrimen.pdf> (Consultado el viernes 27 de julio de 2012).
- 15).- Pérez Wong, Miguel Ángel. **“QUÉ ES LA PROSPECTIVA? DEL MITO A LA REALIDAD SOBRE LA CONSTRUCCIÓN DEL FUTURO”**. Dirección electrónica: <http://catedradh.unesco.unam.mx/catedradh2007/SeguridadHumana/prospectiva%206/revista/numero%203/construf/conspira/wong.htm> (Consultado el viernes 27 de julio de 2012).
- 16).- Rodríguez Vázquez, José de Jesús. **“EL FUTURO AYER Y LA PROSPECTIVA HOY, PARA EL MAÑANA”**. Dirección electrónica: <http://catedradh.unesco.unam.mx/catedradh2007/SeguridadHumana/prospectiva%206/revista/numero%203/construf/conspira/jesus.htm> (Consultado el viernes 27 de julio de 2012).
- 17).- Stern, Jessica (2001): **“EL TERRORISMO DEFINITIVO”** Ediciones Granica, S.A. ISBN: 84-7577-899-2. Impreso en España publicada por acuerdo del editor original.
- 18).- Wilkinson, Paul: **“Political Terrorism”**, Macmillan, Londres, 1974.
- 19). - Wittgenstein, Ludwig. **“Tractatus Logico-Philosophicus”**. URL: <http://www.philosophia.cl/biblioteca/Wittgenstein/Tractatus%20logico-philosophicus.pdf> (Consultado el viernes 27 de julio de 2012).

APÉNDICES

ACERCA DE LA CRIPTOGRAFÍA

"Es dudoso que el género humano logre crear un enigma que el mismo ingenio humano no resuelva".
Edgar Allan Poe.

La protección de la información se lleva a cabo variando su forma. Se llama cifrado (o transformación criptográfica) a una transformación del texto original (llamado también texto inicial o texto claro) que lo convierte en el llamado texto cifrado o criptograma. Análogamente, se llama descifrado a la transformación que permite recuperar el texto original a partir del texto cifrado.

El objetivo de la criptografía es el de proporcionar comunicaciones seguras (y secretas) sobre canales inseguros. Ahora bien, la criptografía no es sinónima de seguridad. No es más que una herramienta que es utilizada sobre la base de mecanismos de cierta complejidad para proporcionar no solamente protección, sino también garantizar que haya confidencialidad. Surgió históricamente por la necesidad de esconder información a los enemigos durante las batallas que se realizaban desde tiempos inmemoriales, hoy en día estas batallas se nos suelen presentar al transitar datos en Internet. En la actualidad, la criptografía es la herramienta fundamental para el desarrollo y estabilidad del comercio electrónico.

Desde la antigüedad hasta la era actual, los mensajes cifrados han jugado un papel destacado en la Historia. Tanto en la milicia, diplomacia y el espionaje, constituyen la mejor defensa de las comunicaciones y datos que viajan por redes de cómputo y por Internet. Hoy en día constituyen un mecanismo de vital importancia para las transacciones de carácter financiero como lo son las compras seguras en la red.

Desde que el hombre ha necesitado comunicarse con los demás ha tenido la necesidad de que algunos de sus mensajes solo fueran conocidos por las personas a quien estaban destinados. La necesidad de poder enviar mensajes de forma que solo fueran entendidos por los destinatarios hizo que se crearan sistemas de cifrado, de forma que un mensaje después

de un proceso de transformación, lo que llamamos cifrado, solo pudiera ser leído siguiendo todo un proceso.

En los procesos de almacenamiento y transmisión de la información es de primordial importancia la seguridad. En el almacenamiento, el peligro latente suele ser el robo del soporte del mensaje o simplemente el acceso no autorizado a esa información, mientras que en las transmisiones lo es la intervención del canal.

La palabra criptología proviene de las palabras griegas *krypto* y *logos* y significa estudio de lo oculto. Una rama de la criptología es la criptografía (de *krypto* y *graphos* que significa descripción), que se ocupa del cifrado de mensajes. Esta se basa en que el emisor emite un mensaje en claro, que es tratado mediante un cifrador con la ayuda de una clave, para crear un texto cifrado. Este texto cifrado, por medio del canal de comunicación establecido, llega al descifrador que convierte el texto cifrado, apoyándose en otra clave, para obtener el texto en claro original. Las dos claves implicadas en el proceso de *cifrado/descifrado* pueden ser o no iguales dependiendo del sistema de cifrado utilizado.

Se entiende por *criptología* el estudio y práctica de los sistemas de cifrado destinados a ocultar el contenido de mensajes enviados entre dos partes: emisor y receptor. La criptografía es la parte de la criptología que estudia como cifrar efectivamente los mensajes.

La *encriptación* es un conjunto de técnicas que intentan hacer inaccesible la información a personas no autorizadas. Por lo general, la encriptación se basa en una clave, sin la cual la información no puede ser descifrada. El National Institute of Standards and Technology de los Estados Unidos ha homologado una norma de codificación denominada *DES (Data Encryption Standard ó norma de cifrado de datos)*.

La criptografía, de acuerdo con la Real Academia Española, es la técnica de escribir con claves secretas o de un modo enigmático. En informática se define como "el arte y la ciencia de mantener seguros archivos y mensajes". Se usan los términos *codificar/descodificar* y *cifrar/descifrar* como sinónimos de *encriptar/desencriptar*.

Encriptar datos tiene dos principales objetivos: la confidencialidad, para mantener la información en secreto, y la integridad, para evitar que la información se destruya o sea corrompida.

El *criptoanálisis* es el arte y la ciencia de transgredir y decodificar un texto encriptado, sin conocer las claves de acceso. La *criptología* es la rama de las matemáticas relativa a la criptografía y el criptoanálisis.

El sistema de mercado capitalista ha transformado el valor de uso con el que inicialmente surge Internet en valor de cambio. Nuestra identidad se convierte en nuestro propio aval, la persona en gran medida se convierte en dinero. Desde que esto sucede, surge la necesidad urgente de la criptografía para proteger los datos confidenciales.

ANTIVIRUS IN MEMORIAM

¿Quién no los recuerda?...

Estamos hablando de 1995 a 1998, aproximadamente.

ANYWARE y THUNDERBYTE, que con su heurística detectaban como posible virus desconocido, los archivos de Word con una fecha alterada -por ejemplo año 2098 cuando el dato real era 1998. También eran capaces de remover el supuesto virus con solamente corregir la fecha. Algo que también podías hacerlo sin ningún antivirus, simplemente ejecutando Norton Disk Doctor.

Obviamente, tal virus desconocido no existía. Quizá se trataba de una fecha alterada por otro virus que ya había sido removido, pero sin corregir esos pequeños daños.

DR. SOLOMON, que con su maravilloso Magic Bullet, podía remover casi cualquier virus sin problemas. Aunque la heurística de este antivirus era un enigma, todos solíamos confiar en ella, pero pocos comprendíamos por qué funcionaba. Muchos especialistas consideran que es el mejor antivirus que haya existido, pero no sabemos cómo fue que McAfee no supo aprovechar toda su grandeza, parece ser que sólo acopló parte de su tecnología.

PC-CILLIN (de Trend Micro) que detectaba muchos virus raros, pero también tenía muchos falsos positivos, consideraba el arranque del Magic Bullet como posible virus desconocido en el sector de arranque y si lo limpiaba, hacía que éste ya no funcionara correctamente.

NORTON (de Symantec), que tenía un montón de discos de rescate -y cada vez aumentaban más-, con su famosa cuarentena, que era como tener un leprosorio en el traspasio de la casa. Pero, uno gustaba más del uso de las Norton Utilities.

F-PROT o COMMAND ANTIVIRUS CON F-PROT –primer antivirus heurístico en la historia de la humanidad-, posiblemente lo más destacado sea su capacidad de detección para las

puertas traseras. También, su famoso F-Macrow, muy bueno para los virus de macro, donde McAfee todavía dejaba residuos al limpiarlos (que de hecho también desarrollaron una herramienta alterna para estos casos).

PANDA ANTIVIRUS, que en sus inicios no detectaba la presencia de virus de macro -o sus remanentes- en archivos temporales-, mientras que McAfee y F-Macrow si lo hacían.

MCAFEE, que todavía continúa dando muchos falsos positivos con su heurística, sobre todo en archivos que en realidad están corruptos (conteniendo un virus que no funciona o solamente remanentes del mismo). Tenía muchos comandos de MS-DOS para limpiar de diversas formas.

En México, se vendía como herramienta adicional el KILLER (atribuido a un programador de apellido Orbe), que servía para limpiar virus triviales, que McAfee solamente detectaba (podía borrarlos pero no removerlos, tales como el famoso virus de la pelotita).

Si queremos ir un poco más atrás, recordamos que McAfee se le llamaba simplemente Scan, era lo primero que llegó a México y parecía no tener competencia -y si la tenía, a nadie realmente le interesaba-, para todos era muy eficiente y era rarísimo que llegara a fallar.

AVP, hoy conocido como KAV (Kaspersky Antivirus), que parecía ser un poco superior a los demás cuando Dr. Solomon fue absorbido por Network Associates Inc. (cuyo producto antivirus era el McAfee. Había una leyenda urbana -nunca supe que tan verdadera fuese, pero posiblemente lo era- que hacía referencia a que las demás empresas tenían a la mano su cajita de AVP para analizar las nuevas muestras que les llegaban de sus clientes, antes de enviarlas a sus laboratorios, y que muchas veces al darse cuenta que AVP las detectaba o "medio detectaba", consideraban el problema como algo real y se apuraban a dar una solución.

Para quiénes saben algo de Antivirus, los corazones palpitan fuertemente al recordar nombres tales como: Allan Solomon, John McAfee, Friðrik Skúlason, Vesselin Bontchev y Eugene Kaspersky (no sé con sinceridad, si deba incluir a Peter Norton).

En la actualidad también se habla de personas tan brillantes como el CEO de ESET, Anton Zajac y su maravilloso equipo, que impulsan su famoso Nod32 y su suite Smart Security, que llegaron a México después del 2000. Se trata de un producto depuradísimo, capaz de competir -bien librado- con todos los demás.

Siento nostalgia por esta época...

Hoy en día, sería muy interesante tratar de hacer prospectiva del mundo de los antivirus y de la seguridad informática, comenzando con pensar seriamente en los posibles escenarios...

CÓMO SE ELABORA UNA BUENA CONTRASEÑA

“Un *password* debe ser como un cepillo de dientes. Úsalo cada día; cámbialo regularmente; y NO lo compartas con tus amigos.” Cristian F. Borghello.

Cabe señalar la importancia de fortalecer nuestras contraseñas y asegurarnos de mantenerlas siempre como algo verdaderamente confidencial. Uno de los errores más comunes es elaborar una clave que sea fácil de recordar (con la intención de no olvidarla), pero no es recomendable basarnos en datos personales (teléfono, número de cartilla, fecha de cumpleaños, etc.), palabras de diccionario (en ningún idioma), nombres de nuestras mascotas, aficiones o gustos.

Si una contraseña se adivina fácilmente, pierde su validez para proteger el acceso a información que se quiere mantener de manera confidencial o reservada. La contraseña ideal es la que usted como usuario puede recordar con facilidad, pero que nadie más pueda dar con ella.

Antes de sugerir reglas para elaborar buenas contraseñas, asegurémonos de poner énfasis en el aspecto de preservar la confidencialidad. Para ello: No comparta sus contraseñas, cámbielas con frecuencia, no las repita en diferentes sistemas, no las almacene por comodidad en su computadora, no la envíe por correo electrónico ni por mensajero instantáneo y, en caso de que intuya que alguien más ya las sabe, proceda a cambiarlas de inmediato.

Además, las contraseñas son vulnerables al robo por tres factores: primero, porque los usuarios acostumbran a ser descuidados, de forma que a menudo escogen contraseñas fáciles de adivinar, segundo, por la forma en que los sistemas operativos guardan, codifican y transmiten las contraseñas y, tercero, los ataques que se pueden realizar a un archivo con contraseña a fin de dar con ella valiéndose de varios recursos. Puntualizamos que, para proporcionar servicios de autenticación, un sistema operativo debe almacenar las contraseñas de manera que pueda compararlas con las que introducen los usuarios en la pantalla de inicio de sesión. Además, un sistema operativo debe transmitir a una computadora remota algo parecido a una clave o código descifrable cuando autentifica una petición de conexión de un usuario remoto. La autenticación deja abierta la posibilidad de que un intruso pueda recuperar

las contraseñas de los usuarios al acceder al archivo de contraseñas o intervenir los canales de comunicación.

Ahora bien, después de haber señalado todo lo anterior, pasemos a señalar varias reglas y sugerencias que los expertos han recomendado en los últimos años para elaborar una buena contraseña (decidimos aquí “caminar sobre hombros de gigantes”). A saber:

- 1.- Debe contener al menos 8 caracteres y no más de 64. Se recomienda combinar números y letras en mayúscula y minúscula, de preferencia no repetir los mismos caracteres. La contraseña distingue mayúsculas y minúsculas, por ello deberá de recordar las letras que escribe en mayúscula. En caso de incluir caracteres que no sean alfa-numéricos hay que averiguar primero cuáles son los que el sistema permite.
- 2.- Nunca utilice una contraseña que resulte fácil de averiguar, fecha de nacimiento o el nombre de sus hijos. Su contraseña no debe contener su nombre de correo electrónico, sus apellidos o la respuesta a su pregunta secreta. Tampoco se deben de utilizar derivados de estos, ni datos personales que se puedan llegar a indagar fácilmente.
- 3.- Nunca escriba su contraseña en papel. Elija una contraseña que pueda recordar (la contraseña debe de ser fácil de recordar para no tener que escribirla y también es deseable que se pueda escribir rápidamente sin necesariamente tener que mirar el teclado, o bien, no tener que depender demasiado de este hecho).
- 4.- No utilice palabras de diccionario en ningún idioma. En la actualidad existen muchos programas para tratar de develar claves que basan su ataque en técnicas de diccionario y de fuerza bruta.
- 5.- Nunca envíe su contraseña por correo electrónico o en un mensaje instantáneo (obviamente tampoco mencionarla en una conversación telefónica, ni faltar a la discreción de manera alguna).
- 6.- No se recomienda poner la misma contraseña en todas partes. Esto es, evite usar exactamente la misma clave en distintos sistemas y archivos.
- 7.- Procure no mantener sus contraseñas indefinidamente. Trate de cambiarlas con cierta regularidad.
- 8.- Existen varias maneras de plantear una contraseña que no sea débil. Por ejemplo, utilice las primeras letras de una frase u oración que no sea tan conocida (puede combinarla con

números o letras), o bien, se puede elegir palabras sin sentido pero que sean pronunciables, etc.

9.- Si se trata de una contraseña para acceder a un sistema procure que esta solamente admita un número limitado de intentos y se bloquee. En caso de que esto suceda frecuentemente, que también pueda enviar un aviso al administrador.

Todas las recomendaciones anteriores van más bien orientadas a los usuarios promedio. En lo que concierne a los administradores de sistemas, considero que ellos están obligados tanto al sentido común como a la preparación necesaria antes de adquirir la responsabilidad de administrar algo y, a la disposición para aprender cada día cosas nuevas e ir las implementando.

HEURÍSTICA DE LOS ANTIVIRUS

Las técnicas heurísticas nacen de la necesidad de una “detección genérica” de los virus informáticos. Se llama detección genérica a la posibilidad de detectar “cualquier virus” aún sin haberlo analizado antes y sin estar en la base de datos del antivirus que se esté considerando. Esto pareciera que carece de sentido pero es tan simple como buscar “instrucciones comunes” de los virus para advertir de la posibilidad de que un archivo o programa esté infectado. .

Cuando analizamos las primeras instrucciones de cualquier archivo, veremos instrucciones para detectar los parámetros de la línea de comandos, borrar la pantalla, llamar a alguna función, ejecutar alguna macro, etc. No obstante tratándose de un virus suelen ser otras bien diferentes como activar el cuerpo del virus o buscar más archivos para intentar implantarles su código.

La experiencia es sin duda lo que lleva a una persona a reconocer algo infectado de algo limpio en cuestión de segundos. Esa “experiencia” se ha pretendido introducir en los programas antivirus bajo el nombre de “heurística”.

El funcionamiento de la heurística es sencillo, primero se analiza cada programa sospechoso sin ejecutar las instrucciones, lo que hace es desensamblar o "descompilar" el código de máquina para deducir que haría el programa si se ejecutara. Avisando que el programa tiene

instrucciones para hacer algo que es raro en un programa normal, pero que es común en un virus.

Sin duda el principal problema de las técnicas heurísticas ha sido los falsos positivos. A pesar de que se han mejorado mucho en los últimos años, siguen sin conseguir demasiada efectividad (aunque hay algunas excepciones). El problema más que en la calidad de la rutina heurística está en la interpretación que el usuario realice de ese aviso heurístico. Si es poco experimentado estará constantemente mandando muestras a su casa de antivirus ya que “el antivirus le dijo que podía tener un virus”.

Entendiendo la Heurística como un indicador de probabilidad de contagio, esto nos lleva a considerarla como un sistema de detección mejorada que al incluirla los antivirus nos permite establecer un sistema de alerta y de prevención ante la aparición de mutaciones de virus o de nuevos virus.

Esta técnica permite "barrer" diferentes tipos de códigos dentro de los archivos, que sean susceptibles de ser malignos. Códigos que son genéricos dentro de los archivos maliciosos y que siempre suelen ser parecidos. O por lo menos respetar parte de las cadenas de comandos que activan los virus.

Pero ¿cómo opera un antivirus? Los virus tienen patrones de códigos que son como sus "huellas digitales". Los software antivirus buscan estos patrones, pero sólo de los que tienen almacenados en su lista (por esto la actualización es tan importante). Estos productos también pueden valerse de la heurística, es decir, analizan los archivos para detectar comportamientos similares a los de los virus.

Cada día crece el número de nuevos virus y la alternativa para poder neutralizarlos, sin haber programado antes el antivirus para su reconocimiento, es la denominada “búsqueda heurística”. A través de ella, el programa antivirus analiza el código de los programas buscando instrucciones, acciones sospechosas o indicios que delaten la presencia de virus en la computadora, de acuerdo a los patrones habituales empleados por los códigos maliciosos.

El método Heurístico es una tecnología de programación que dentro de sus rutinas de detección de especies virales, incluye las cadenas clásicas que son similares, parecidas o afines a virus auténticos. El método heurístico, si no está bien programado, es susceptible de incurrir en resultados falsos positivos o negativos. Además, al encontrar un virus desconocido,

variante de otro existente, el antivirus que emplea este método de búsqueda no podrá eliminar eficientemente el virus y mucho menos reparar el archivo o área afectada.

Para que un antivirus detecte y elimine eficientemente a un virus así como también repare los daños ocasionados, debe incluir en la base de datos de sus rutinas de detección y eliminación el exacto micro código viral de esa especie. Sin embargo la técnica de búsqueda heurística de virus por "familias" es una forma eficiente de detectar a especies virales que pertenecen a una misma familia, aunque no es un método absolutamente exacto o eficiente.



Prof. Arnaldo Moreno Pérez

miru@prodigy.net.mx

arnaldo_58@hotmail.com

amorenop@ipn.mx

Promotor Especializado de la Dirección General del Instituto Politécnico Nacional.

Profesor de Matemáticas del Instituto Comercial Mendoza A.C. (<http://www.institutomendoza.edu.mx/>).

Consultor Independiente en Seguridad Informática, Prospectiva Estratégica y Comunicación Social.

Cybermedios, innovación y presencia digital para su empresa
<http://emprendedores.cybermedios.org/>
http://emprendedores.cybermedios.org/?page_id=47).

- Mexicano. Nació el 24 de enero de 1958 en Monterrey, Nuevo León. Actualmente vive en la Ciudad de México, Distrito Federal.
- Realizó estudios de Maestría en Ciencias en la Especialidad de Matemáticas en el Centro de Investigación y Estudios Avanzados del Instituto Politécnico Nacional (1982), y de Licenciatura en Ciencias de la Comunicación con Especialidad en Comunicación Política (2005-2011) en la Facultad de Ciencias Políticas y Sociales de la Universidad Nacional Autónoma de México (UNAM).
- Ha sido Profesor de Matemáticas, Física, Historia y Teorías de la Comunicación, en los niveles de Bachillerato y Licenciatura, en instituciones tanto públicas como privadas.
- Se ha desempeñado como Servidor Público en la Secretaría de Programación y Presupuesto (1989-1991), Secretaría de Hacienda y Crédito Público (1992-1994), Secretaría de Comunicaciones y Transportes (1995-2003) y en el Instituto Politécnico Nacional del 2004 hasta la actualidad.
- Colaborador en varios medios digitales (<http://www.virusattack.com.ar/>, <http://monografias.com>, <http://www.vsantivirus.com>, <http://www.virusprot.com>, <http://www.segu-info.com.ar>, <http://www.emprendedoras.com>, <http://www.seguridadydefensa.com/>, <http://www.zonavirus.com/>, etc.)
- Conferencista de talla internacional: B-Secure, ASIS International, UNAM, UNISON, IPN, ITESM, etc. Asesor independiente en Virus y Antivirus, quizá uno de los más reconocidos en América Latina, España y Portugal. Empezó en el año 2003 el primer ciberchat en español sobre virus informático, auspiciado por el Instituto Nacional de Estadística Geografía e Informática.
- Consultor en Seguridad Informática de la Facultad de Ciencias Políticas y Sociales de la UNAM.

COMENTARIOS EN TORNO A ESTA OBRA Y SU AUTOR:

“Arnoldo es un personaje al cuál le reconozco su madurez y persistencia en la materia de Seguridad Informática; ya que ha sido uno de los pioneros en entender el significado de la palabra “Seguridad”. Tengo muchos años de conocerlo y cada día que pasa me sorprende más por su capacidad de mantener actualizados sus conocimientos en la materia y sobre todo por compartir desinteresadamente sus vivencias que nos llevan a tener un margen más amplio en cuestiones de informática y su seguridad.” **Ing. Clemente Topete**. Profesional de la Seguridad Informática y Catedrático del Posgrado de Diseño Industrial en la Facultad de Arquitectura de la UNAM (clemente_topete@hotmail.com).

“El Mtro. Arnoldo Moreno, nos ofrece un libro que sin duda llegara a revolucionar el mundo de la seguridad informática, sus publicaciones e investigaciones le han otorgado la experiencia y reconocimientos, en el ámbito internacional por sus contribuciones en seguridad informática.

Ha trazado una amplia carrera en este ámbito considerándose como uno de los pioneros en investigación cibernética de seguridad, incansable en la búsqueda de nuevos ataques cibernéticos y la manera más inteligente por medio de las matemáticas aplicadas para combatirlos.

La inseguridad informática y el cibercrimen es la nueva cara de la delincuencia organizada, teniendo como armas el poco conocimiento sobre herramientas de protección y la vulnerabilidad de la tecnología. Los sectores que llegan a tener mayor incidencia se encuentran los servicios financieros y gobierno, pero el usuario promedio con la llegada de los correos spam, phishing, etc., también es víctima en una proporción menor. Sin duda este libro otorgara todos los trucos y puntos interesantes para combatirlo, pero sobre todo mantenernos informados sobre este nuevo tipo de delincuencia.

Considero humildemente que el Mtro. Arnoldo Moreno, *es un guerrero que está en continua búsqueda de algo sin siquiera saber que es, que busca mejorar y cambiar aun cuando eso vaya en contra de lo que la sociedad y el sistema ha impuesto como normal y aceptable, que confía y cree más allá de lo que sus ojos pueden ver, muchas veces siente estar en el lugar o planeta equivocado pero que a la vez intuye que fue una elección propia estar aquí para responder por mas difícil que sea*

Duda y confía a la vez, pues a veces siente miedo pero al final siempre se convence de que no hay nada que temer, que quiere cambiar al mundo pero sabe que debe tener paciencia y tolerancia, que sabe que no todos debemos librar las mismas batallas aun cuando la manera de ganarlas es la misma.. Conciencia plena y amor incondicional hacia todo lo que forma parte de sus convicciones incluyendo a nosotros mismos.

Sin importar las batallas libradas, ganadas o perdidas, siempre se levanta.”

Ing. Zidzielia Ibarra, Consultor Financiero y Tecnológico. *Fulkrum*, Colocación Privada de Obligaciones, Hamburgo 227, Colonia Juárez, México, D.F. (zibarra@fulkrumoperadora.com).