

EVALUACIÓN DE LAS PREDICCIONES EN SEGURIDAD DE LA INFORMACIÓN PARA EL 2009 Y EL RIESGO DE LAS PREDICCIONES PARA EL 2010

Por: Jeimy J. Cano, Ph.D, CFE

El año 2009 será recordado como un año de transición, reconversión de acciones y ajustes de acuerdo con los riesgos inherentes de los diferentes sectores productivos del mundo. Este año que culmina, nos deja con muchas enseñanzas, entre otras, que la variabilidad del mundo está a la orden de día y que de aquí en adelante, deberemos ser mas cuidados, más focalizados, pero sobre manera, más activos y visionarios, para lanzarnos a conquistar nuevos retos y experimentar nuevas posibilidades, siempre en un marco de riesgos calculados, proyecciones propositivas y acciones concretas.

Al igual que se adelantó el año anterior, revisaremos si las predicciones ilustradas para este 2009 se ajustaron a la realidad de lo ocurrido y confrontar con hechos y revisiones lo que se dijo al inicio de estos 365 días. Así mismo, se presentarán algunas tendencias propias que se observaron a lo largo del año, que no fueron parte del ejercicio realizado al finalizar el año 2008 y que se hicieron evidentes durante el 2009.

Finalmente intentaremos, hacer un ejercicio de predicción, bastante arriesgado por cierto, que nos lleve a visualizar un poco lo ocurrido en estos primeros diez años del nuevo milenio y lo que se puede vislumbrar en el horizonte para el año 2010. El año 2010 es un año particularmente especial, pues cierra una primera década de este milenio y abre un nuevo momento. Por tanto, lo que aquí se plantea es una doble responsabilidad para los encargados de la seguridad de la información, aprender de lo que hemos recorrido y abrir nuestro entendimiento para entrar en la dinámica de la inseguridad que promete mantenernos alerta y despiertos en este nuevo camino.

PREDICCIONES DEL 2009

A finales de 2008, se adelantaron reflexiones sobre cómo se podría comportar la inseguridad de la información, basadas en análisis y tendencias que se observaban en ese momento. Si bien se presentaron sucesos que confirmaron las mismas, se manifestaron otros desafíos que nos pusieron atentos y que se comentarán brevemente en esta revisión.

Predicción No.1- Inseguridad en ambientes virtualizados

Análisis: ***** Durante el 2009, los ambientes virtualizados ganaron un espacio muy importante en las agendas de los ejecutivos de tecnologías de información. La promesa de hacer más rentable la inversión en infraestructura y ganar flexibilidad en su configuración, llevó a muchas organizaciones a tomar esta opción para mejorar el retorno de la inversión en tecnología. Sin embargo, este logro, se enfrenta a nuevos retos que apenas inician y que darán de que hablar los próximos años, uno de ellos la computación en la nube.

Infraestructura, plataformas operacionales y aplicaciones que ahora estarán en todas partes, administradas y soportadas por terceros, basadas en un modelo de demanda de servicios, donde los datos y la información serán los que se “mueven” de un lugar para otro, según se requiera para mantener el balance costo/beneficio y el rendimiento requerido y esperado por los clientes.

Predicción No.2 - Identificación y desarrollo de una inseguridad convergente

Análisis: *****Al igual que la predicción anterior, este vaticinio está aún en sus inicios. La promesa de un mundo integrado, convergente y multilinguaje apenas despega. De acuerdo con la ITU (*International Telecommunication Union*), estas redes funcionales de multiservicios, con la capacidad de diferenciar usuarios y servicios a través de políticas de calidad bien definidas, tienen varios años aún de desarrollo, sin perjuicio de que tecnologías emergentes poco a poco hagan su aparición precipitando la materialización de una inseguridad convergente, que debe mantenernos atentos y dispuestos a revisar las viejas técnicas de ataque, como referente base para analizar y las posibilidades asociadas con mutaciones de plagas informáticas actuales, ahora en un contexto integrado y multiprotocolo.

Predicción No. 3 - Reinención del responsable de la seguridad de la información – Chief Security Officer o Chief Information Security Officer-CISO

Análisis: ***** Luego de revisar varias encuestas sobre seguridad de la información publicadas durante el 2009, se observa una clara tendencias de los CISO hacia el negocio, hacia las personas, hacia la comprensión de los flujos de información, más que las relaciones y aspectos tecnológicos. Esta posición orientada al negocio, hace que la seguridad cobre una importancia más allá de las máquinas y de las fallas de éstas; es una manera de advertir, que el eslabón más débil de la cadena finalmente se ha identificado, se ha hecho evidente. Sin embargo, aún queda mucho por recorrer, por descubrir en el ADN de los nuevos CISO, que conscientes de los riesgos de la seguridad y apalancados en el conocimiento holístico del negocio, deberán ser capaces de enfrentarse al enemigo y maestro, a la razón de ser de su rol: la inseguridad de la información.

Predicción No.4 - Se inicia la era del e-cumplimiento y se activan las fuerzas de lucha contra la ciberdelincuencia

Análisis: ***** No hay duda que el 2009 pasará a la historia como uno de los años donde se acentuaron los cumplimientos de regulaciones y normas. La inestabilidad de los mercados mundiales, provocaron una alerta generalizada y un llamado a los gobiernos y reguladores para monitorear más de cerca lo que ocurre. Este llamado necesariamente enfrentó a las áreas de tecnologías de información y a las de negocio en la encrucijada de crecer y regular al mismo tiempo. Con este escenario, la inseguridad de la información encontró otro motivador para hacer más exigente la responsabilidad del gerente de seguridad y mostrar que es capaz de mimetizarse en las relaciones de negocio, combinando las malsanas inclinaciones humanas, las facilidades tecnológicas y las tendencias dispares del mundo político, económico, social y científico.

Predicción No. 5 - Habrá mayor atención a los logs y su correlación

Análisis: ***** Es probable que los registros de seguimiento (o *logs*) hayan tenido una mayor preponderancia durante 2009, dado que múltiples eventos de seguridad de la información se presentaron, los cuales requirieron un análisis detallados de los mismos. Sin embargo, las preguntas de fondo permanecen: ¿son confiables?, ¿son confiables las herramientas que los producen?, ¿no han sido manipulados por terceros?, ¿tenemos forma de verificar su integridad?, preguntas que en el fondo hacen un llamado a los administradores de la infraestructura para hacer de la seguridad de la información, no un criterio más dentro de su plan de capacidad, sino la variable que articule sus esfuerzos de dimensionamiento para el futuro.

PREDICCIONES PARA 2010

Cada vez se hace más exigente tratar de predecir qué pasará con las tendencias de la inseguridad en los años venideros, pues su movimiento no probabilístico y disímil, deja en evidencia al mejor analista que trate de modelar sus inciertos patrones y describir las líneas poco visibles de su trayectoria.

Considerando lo anterior y con la alta probabilidad de andar por sendas poco conocidas, trataremos de visionar las variaciones y efectos de la inseguridad de la información considerando las tendencias actuales de los eventos que se han manifestado hasta el momento y prometen seguir en el 2010.

A continuación cinco predicciones de lo que puede pasar durante 2010 en temas de inseguridad de la información.

1. Tormentas en la nube

Nuestra *huella digital* (datos que nosotros mismos generamos en sitios web, redes sociales, blogs, entre otros) (IDC REPORT 2008) cada vez es más amplia y visible. Ahora en un contexto de computación en la nube, donde tenemos una visión distribuida y de multiservidores virtualizados, es posible tener una *sombra digital* (información sobre nosotros) cada vez más extendida, difusa y muchas veces distorsionada, que impacte directamente los temas de seguridad y privacidad tanto de los datos como de la información.

Ante esta realidad, que de acuerdo con un estudio reciente de IDC, se espera que la inversión en este tipo de servicios crezca un 27% para 2012, es decir una inversión de 42 billones de dólares, (MATHER, T., KUMARASWANY, S. y LATIF, S. 2009, pág.10) es evidente que iniciativas como la de la *Cloud Security Alliance* animen las reflexiones y discusiones de las diferentes implicaciones de este tipo de tendencias que pone de manifiesto una computación basada en servicios de infraestructura, plataforma y aplicaciones.

2. Inseguridad móvil: equipos, datos e información

La realidad de los dispositivos móviles es contundente. Las cifras manejadas por Canals (2009) sobre el mercado de teléfonos inteligentes donde se muestra un crecimiento de 4% año con año de estos dispositivos, llegando a una cifra de 41.4 millones de unidades en el tercer cuarto de 2009, así como el despacho de estas unidades con servicios integrados como GPS y WI-FI, nos muestran que habrá mayores elementos que analizar y proteger en la computación móvil.

Esta tendencia, sumada al hecho que no se cuentan con adecuadas medidas de aseguramiento y control en este tipo de dispositivos (MAISTO 2009), nos abre un panorama bastante inestable y exigente para mantener el nuevo perímetro extendido de las organizaciones. Adicionalmente, la tendencia creciente del uso de memorias o dispositivos USB (más de 860 millones de unidades despachadas en 2007, considerando un crecimiento de 15% para 2010 según estudio reciente de Gartner – JUNGO 2009), se mantiene y extiende la alerta de fuga y pérdida de información en las organizaciones, lo que implica un ejercicio estratégico de los responsables de la seguridad de la información por incorporar prácticas de aseguramiento de información adecuadas con los flujos de información de negocio.

3. Cultura de la inseguridad: Desobediencia del factor humano

Considerando las reflexiones efectuadas por Furnell y Thomson (2009) en su documento de febrero de 2009 sobre la desobediencia de los usuarios para aceptar las medidas de seguridad de la información, es claro que las estrategias de sensibilización e interiorización de la seguridad, sigue siendo un reto importante para las áreas de seguridad de la información.

Mientras la seguridad de la información siga siendo un elemento externo la cultura de la organización, que no se contemple como parte fundamental de los procesos de negocio, basado en los flujos de información articulados en las soluciones de tecnología y adicionalmente, se advierta como “algo” que hay que cumplir por regulación o mandato normativo, las iniciativas de seguridad de la información serán objeto de apatía, desobediencia y resistencia. En este contexto, se genera un campo abonado para que la inseguridad riegue con serenidad sus nuevas semillas, esperando sin mayores contratiempos que nuevas manifestaciones hagan su aparición tanto en la tecnología, como en los procesos y las personas.

4. Nuevos retos, nuevas habilidades: Ciberseguridad, forensia y administración de riesgos

Ante una realidad de tecnologías de información y comunicaciones basadas en temas como computación en la nube, tecnologías convergentes, movilidad, perímetros porosos y plagas informáticas extendidas (redes sociales y teléfonos inteligentes), se requiere que los profesionales de la seguridad de la información desarrollen nuevas habilidades (GUPTA 2009, FIELD 2009) que permitan enfrentar esta realidad y apalancar las mismas en una

cultura de seguridad de la información que genere una “barrera” importante para los atacantes y sus pretensiones.

La administración de riesgos, ya no es un ejercicio corporativo o específico efectuado para validar un contexto específico de un tema, tecnología o proceso, sino una competencia organizacional de cada uno de los individuos, que permita mantener un nivel de riesgos conocido, basado en prácticas confiables de administración de activos de información. De manera complementaria, dichas prácticas confiables, deberán estar como valores en uso (en todos los individuos de la organización) que muestren una relación adecuada con los servicios expuestos en internet y la información que se comparten allí.

Finalmente y no menos importante, cuando se materializa una falla de seguridad o peor aún, se hace evidente un fraude, se requiere que este profesional cuente con las habilidades requeridas para identificar, recoger, analizar y presentar los elementos materiales probatorios que sustenten las pruebas requeridas ante procesos jurídicos que se deriven de la atención de incidentes o actos ilegales. (CANO 2009) Esto no es otra cosa, que se cuente con destrezas propias de la computación forense que permitan avanzar rápidamente en la contención y análisis de lo ocurrido.

5. Las bases de datos: “la joyas de la corona en jaque”

El almacenamiento de los datos e información siempre es materia de análisis y revisiones en las organizaciones del siglo XXI. Un reciente estudio de ESG Research (ESG RESEARCH 2009), sobre las bases de datos, nos muestra que un alto porcentaje de ellas dependen de procesos manuales y que no cuentan con apropiadas medidas de seguridad, de acuerdo con la información, generalmente catalogada como confidencial, que permanece en ellas.

Así las cosas, la fuente principal, el insumo básico para el funcionamiento de las organizaciones y sus procesos de toma de decisiones, se encuentra en una ruta de malas prácticas y procesos poco automáticos que hacen encender las alarmas de los responsables de la seguridad de la información, para iniciar un proceso de aseguramiento que permita ajustar un paso más en su estrategia metodológica de defensa en profundidad.

Si bien esta tendencia en las bases de datos no es nueva, a lo que si apunta esta predicción, es a advertir que no es posible seguir aplazando este proceso de aseguramiento, de integración con las características de seguridad de las aplicaciones y por qué no, hacer este ejercicio parte inherente y fundamental de la arquitectura de tecnología de información y comunicaciones de las compañías.

CONCLUSIONES

Hacer este ejercicio año con año y confrontarnos a nosotros mismos frente a lo que sugerimos que sucedería el año en curso, es una reflexión que nos confronta desde múltiples perspectivas, buscando hacer el mejor esfuerzo para encontrar en la aparente aleatoriedad de la inseguridad, la lógica de la falla que nos permita distinguir realidades

emergentes y posibles acciones frente a éstas. En este contexto, este documento es una invitación para revisar las agendas de los ejecutivos de tecnologías de información, responsables de la seguridad de la información y directivos de empresas, como una excusa académica y práctica para ver la práctica de la seguridad en el contexto de negocio y la generación de valor para sus grupos de interés.

La seguridad de la información es un proceso exigente y dinámico que requiere la habilidad para mantener en movimiento constante el ojo crítico de su responsable frente a la inseguridad, no sólo para crear la sensación de confiabilidad requerida por los usuarios del sistema, sino para que vinculando a estos últimos en la conquista de la no linealidad de la inseguridad, se construya de manera conjunta una distinción real y evidente de un ambiente controlado y confiable, mas no seguro.

Sólo nos queda observar el desarrollo del 2010, para ver cómo la inseguridad de la información nos sorprende y nos hace meditar nuevamente y así, pensar de manera distinta para abrirle la puerta a las posibilidades, esas que no son otra cosa que el insumo del desaprendizaje continuo, virtud de la cual se debe alimentar permanentemente el instinto y la mente del responsable de la seguridad de la información.

REFERENCIAS

CANALYS (2009) Smart phone market shows modest growth in Q. Disponible en: <http://www.canalys.com/pr/2009/r2009112.htm> (Consultado: 13-Dic-2009).

ESG RESEARCH (2009) Frightening database security realities. Disponible en: http://www.guardium.com/assets/PDF/Databases_at_Risk_An_ESG_Research_Brief_Compliments_of_Guardium_2009-09.pdf (Consultado: 12-Dic-2009).

GUPTA, U. (2009) The future of Information Security Profession. Disponible en: http://www.bankinfosecurity.com/articles.php?art_id=1997&opg=1 (Consultado: 13-Dic-2009).

FIELD, T. (2009) Core security skills: What's required in 2010? Disponible en: http://www.bankinfosecurity.com/articles.php?art_id=1976&opg=1 (Consultado: 13-Dic-2009).

JUNGO (2009) USB Market Overview. Disponible en: http://www.jungo.com/st/usb_market.html (Consultado: 13-Dic-2009).

MAISTO, M. (2009) Enterprise cell phone security is lacking, say report. Disponible en: <http://www.eweek.com/c/a/Mobile-and-Wireless/Enterprise-Cell-Phone-Security-Is-Lacking-Says-Report-757731/> (Consultado: 13-Dic-2009).

IDC REPORT (2008) The diverse and exploding digital universe. Disponible en: <http://www.emc.com/collateral/analyst-reports/diverse-exploding-digital-universe.pdf> (Consultado: 13-Dic-2009).

Sin autor. (2009) Horóscopo 2010 para la seguridad informática. Disponible en: <http://www.redusers.com/horoscopo-2010-para-la-seguridad-informatica> (Consultado: 12-Dic-2009).

FURNELL, S. y THOMSON (2009) From culture to disobedience: Recognising the varying user acceptance of IT Security. *Computer Fraud & Security*. February.

CANO, J. (2009) *Computación forense. Descubriendo los rastros informáticos*. Editorial AlfaOmega.

MATHER, T., KUMARASWANY, S. y LATIF, S. (2009) *Cloud security and privacy. An enterprise perspective on risks and compliance*. O'Really.

Datos del Autor:

Jeimy J. Cano, Ph.D, CFE

Ingeniero y Magíster en Ingeniería de Sistemas y Computación de la Universidad de los Andes. Doctor en filosofía de la Administración de Negocios, Newport University, USA. Profesor – Investigador en temas de seguridad de la información, computación forense y evidencia digital. Miembro investigador de la Red Iberoamericana de Criptología y Seguridad de la Información - CriptoRED, Miembro del Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática - GECTI de la Facultad de Derecho, Universidad de los Andes. Es Examinador Certificado de Fraude (CFE) por la ACFE y Cobit Foundation Accredited por ISACA. Autor del libro: *Computación Forense. Descubriendo los rastros informáticos*. AlfaOmega. Contacto: jjcano@yahoo.com