Monitoreo y evolución de la seguridad de la información

Jeimy J. Cano, Ph.D, CFE

Introducción

Estamos ante un mundo marcado por las turbulencias financieras, políticas, sociales y tecnológicas. Una realidad donde la información se ha convertido en el instrumento fundamental para descubrir posibilidades y crear oportunidades; pero de igual manera un arma táctica y estratégica para todos aquellos que desean reservarse un puesto privilegiado en el futuro próximo.

En este contexto las organizaciones han venido revisando el horizonte tecnológico y las posibilidades reales para generar ventajas competitivas, que le permitan mantenerse vigentes y privilegiadas frente a sus inmediatos competidores. En este sentido el informe de Mckinsey (SPANG 2009) establece cinco tendencias que pueden cambiar la forma de los negocios actuales con TI. Estas tendencias son:

• Convergencia entre las finanzas corporativas y el área de tecnologías de información – TI

• Tensiones alrededor del incremento de los presupuestos del área TI

• Los costos en los proyectos de TI

• El incremento de regulaciones para TI

• El *offshoring* (desarrollo con terceros) y *outsourcing* como cambios en la estrategia de TI

Si observamos estas tendencias, podemos advertir que las organizaciones estarán demandando mayores niveles de efectividad operacional y estratégica de las áreas de tecnología, y por otro, abriendo sus límites corporativos para interactuar con terceros, o mejor, posibilitando a sus ejecutivos nuevas experiencias tecnológicas móviles para andar al ritmo de los negocios y los mercados actuales.

En este escenario asistimos a una apertura de los perímetros tecnológicos de las empresas, los cuales van más allá de los límites impuestos por las instalaciones físicas donde se encuentran los equipos de computación; pasando ahora a una movilidad abierta y constante de múltiples dispositivos electrónicos que se encuentran entre las pertenencias de los ejecutivos de las compañías como son entre otros los asistentes portátiles digitales, los celulares inteligentes, los buscapersonas.

Si lo anterior es correcto y la información adquiere mayor movilidad entre diferentes redes de datos, bien sean alámbricas o inalámbricas, la seguridad de la información tradicional, basada en perímetros conocidos y cerrados, requiere una revisión y actualización para ser consecuente con las necesidades de los negocios y ajustarse según la confiabilidad y aseguramiento requerido para mantener el flujo de los procesos y confianza de los accionistas y clientes.

En razón con lo anterior, este documento busca revisar la evolución del concepto de la seguridad de la información frente a la dinámica de los negocios actuales, monitorizar la evolución de las temáticas propias de la gestión de la seguridad, como son entre otras la cultura de seguridad, los requisitos de cumplimiento, la seguridad en las aplicaciones, los incidentes de seguridad, así como el surgimiento del concepto de resiliencia organizacional, como factor vinculante entre la continuidad de negocio y la continuidad tecnológica.

Evolución de la naturaleza de la seguridad de la información (LACEY 2009, págs.15-16)

La información es la base fundamental sobre la cual la seguridad desarrolla su dinámica y propone las acciones de protección. En este sentido, las motivaciones de control y confiabilidad han venido evolucionado con el paso de los años.

En los años 70’s con el nacimiento de los sistema de computación

o *mainframes,* donde se contaban con máquinas de procesamiento de datos centralizados, las características de seguridad se concentraban en controles propios y particulares al hardware y software de los proveedor de dichas tecnologías. En este contexto, firmas como IBM y WANG, daban los lineamientos generales de seguridad y control ajustados a sus equipos, indicando aspectos técnicos de operación, seguridad física, recuperación ante desastres, así como la segregación funcional necesaria para mantener controlada y confiable la operación del sistema.

Con el pasar de los años, en los 80's con el surgimiento de las redes de computadores y un animado flujo de información entre diferentes puntos, las motivaciones de seguridad de la información salen de la máquina central, a un conjunto o colección de máquinas, las cuales generan nuevos retos para los encargados de las tecnologías de información como son entre otros las fallas de la suite de protocolos TCP/IP, las exigencias de las aplicaciones en el entorno cliente/servidor, la administración remota de máquinas, la administración de la infraestructura de seguridad de la información.

Ya para los años 90's con una alta penetración del uso de Internet, con una fuerte demanda de servicios en el web y con un individuo exigente por innovación y productos informáticos en la red, los encargados de TI advierten nuevas motivaciones alrededor del tema de seguridad de la información. Por tanto, con una alta exposición del usuario final a las herramientas y servicios en la red, y un desmedido deseo de explorar y conocer, basado en la aparente confianza que le brinda Internet, la información circula con mayor libertad y las infraestructuras empresariales requieren mayores canales de comunicación y estrategias de protección que antes no eran pensables. Los gusanos, el software espía, los código maliciosos móviles, la suplantación de identidad, entre otros elementos conforman el escenario de plagas informáticas que deben ser atendidas por los especialista en TI.

En lo corrido de la primera década de este nuevo milenio, se advierte un nuevo cambio de foco en la seguridad de la información. Los negocios se mueven en un contexto global, las operaciones se inician en un país y se terminan en otro, las reuniones se hacen de manera virtual y la educación busca espacios de motivación fuera de las aulas. Todo ello implica

que asistimos a una renovación de las condiciones locales de seguridad empresarial, a unas basadas en redes que están más allá del perímetro corporativo.

En este escenario, tenemos un perímetro extendido o poroso que nos reta a ofrecer condiciones de seguridad concretas y viables que balanceen las necesidades de los procesos empresariales y las principios de seguridad de la información: confidencialidad integridad y disponibilidad. En consecuencia, la seguridad de la información pasa de ser un servicio en sí mismo del negocio, a ser parte integral del negocio, pues los riesgos derivados de esta nueva interacción abierta y global, hacen parte inherente de los objetivos corporativos y de las metas grandes y ambiciosas (MEGAS) de las empresas en este entorno.

Las temáticas actuales de la gestión de la seguridad de la información

Con una realidad global e interconectada como la actual, la seguridad de la información basada en manuales de políticas y estándares requiere ser revisada, para evolucionar con las exigencias de un ambiente altamente competitivo, ágil y de alto riesgo propio de las organizaciones que encuentran en las tecnologías de información su factor diferenciador y desestabilizador en su entorno de negocio.

De acuerdo con McAfee (2006), existen tres variedades de tecnologías de información que cambian nuestra manera de trabajar: la TI funcional, la TI de Redes y la TI Corporativa. Cada una de ellas con una definición e impactos propios en la dinámica de las organizaciones. Particularmente nos concentraremos en la TI de Redes, esa que facilita la interacción de las personas sin especificar sus parámetros.

Estas tecnologías facilitan la colaboración entre las personas, permiten expresar las opiniones de ellas y compartir y buscar información que les asista en su constante necesidad de estar informados sobre las temáticas que son de su interés. En este escenario, la inseguridad de la información se materializa en vulneración de la privacidad de la información, la fuga de información sensible, la porosidad de un perímetro extendido y el mal uso de los datos para efectos de inteligencia o actividades ilícitas.

En consecuencia, las organizaciones, de cara a estos nuevos retos que propone la inseguridad, requieren

establecer acciones propias de la gestión de la seguridad que permitan enfrentar y asegurar los riesgos que un escenario interconectado, global, poco regulado, altamente consultado y vulnerable establece para los responsables de la seguridad de la información corporativa. (WILBANKS 2008)

Cultura de seguridad de la información

Un primer elemento y por demás, uno de los más importantes, es la cultura de seguridad de la información. Siguiendo las consideraciones del Dr. Edgar Schein, sobre cultura organizacional, una cultura esta compuesta por tres componentes: los artefactos, lo que se observa (lo que se ve, lo que se siente y escucha), símbolos y comportamientos; los valores expuestos, es decir, lo que le dicen y finalmente, los supuestos básicos, aquello que los participantes dan por hecho. (WESTNEY 2008)

Basado en lo anterior, podríamos decir que cultura es la base fundamental de la gestión de la seguridad, entendida ésta como la promoción inherente y natural de comportamientos confiables de las personas que permitan interiorizar la distinción de prácticas de protección coherentes con las políticas internas, el fortalecimiento de una percepción y administración del riesgo, el convencimiento emocional de una actitud de autocuidado, los impactos financieros de acciones inseguras y sobre manera, el interés y entendimiento propio de las regulaciones que sobre el tema se tienen.

La cultura de seguridad de la información debe ser el animador y custodio de variables tan importantes para las organizaciones como su reputación, los ingresos, el cumplimiento regulatorio, la percepción del cliente y los flujos de información en los procesos.

Los requisitos de cumplimiento (SCHNEIER 2004)

¿Qué podríamos llamar cumplimiento? Es la pregunta que nos surge cuando observamos la creciente demanda de autoridades o entidades de supervisión y control por el cumplimiento de normativas o directivas nacionales o internacionales. Si bien las buenas prácticas son parte inherente de la evolución de la gestión de la seguridad de la información, cada organización, en su dinámica de negocio, debe comprender los riesgos a los cuales se encuentra expuesta y responder de acuerdo con este diagnóstico.

A la fecha las organizaciones, consecuente con los mandatos de los supervisores, requieren satisfacer una serie de requisitos técnicos y administrativos para hacer de su estrategia de seguridad una gestión más confiable y efectiva. Así mismo, se enfrentan al dilema propio de cualquier organización en un mundo en crisis: ¿qué tanta seguridad es necesaria para mi negocio? Una pregunta que exige una comprensión detallada y profunda de las funciones de negocio y cómo la información fluye al interior de sus procesos.

Las respuestas a estas preguntas, manifiestan la necesidad de contar con un sistema de control interno informático que permita la evolución permanente y constante de los sistemas de gestión de seguridad de la información, basados en una administración inteligente de los riesgos, una comprensión de la dinámica de la inseguridad y la validación de los controles actuales que la organización establece para operar de manera confiable. (TANEY Jr. y COSTELLO 2006)

La seguridad de las aplicaciones (CURPHEY y ARAUJO 2006)

Si bien contar con un sistema de control interno informático es factor clave para el mantenimiento de la gestión de la seguridad de la información, las aplicaciones deben estar alineadas en este mismo modelo, un sistema de evolución y aseguramiento de todos y cada uno de sus componentes, con el fin de mitigar posibles efectos de borde no deseados en su operación.

El desarrollo de aplicaciones menos inseguras, es una práctica emergente derivada de las prácticas generales de ingeniería de software. Si bien, no han sido establecidos referentes generales sobre la seguridad del software, la contundencia de los hechos sobre las fallas de los programas, ha hecho que la industria tome conciencia de los mismos y procure hoy mejores soluciones informáticas para las organizaciones.

Es claro que el software sin errores o fallas está muy lejos de la realidad, pero lo que si es claro es que se hace necesario establecer métricas que permitan ubicar un punto en el tiempo para saber dónde estamos y qué tenemos, y los niveles de aseguramiento de información que deseamos para las soluciones tecnológicas futuras.

Los incidentes de seguridad (ETGES y McNEIL 2006)

Como la única constante en el mundo es la inseguridad, la atención de los incidentes es la norma que toda gestión de seguridad de la información debería tener. Considerando que un incidente lo podemos definir como una cadena sucesiva de aplicación de inadecuadas prácticas de seguridad, podemos observar que éstos son eventos que materializan una conciencia colectiva de creencias que responden a un apetito natural al riesgo de las personas y sus acciones.

Por tanto, todos los aprendizajes que de estas realidades podamos obtener, deben beneficiar y fortalecer una cultura de seguridad de la información basada en el reporte abierto y oportuno de las actividades inseguras, la sinceridad y transparencia de las notificaciones de los hechos eventuales y sobre manera, la firme convicción de la organización para prepararse mejor para disminuir los impactos de una falla parcial o total en sus operaciones de negocio.

El reporte de los incidentes es la materia prima para afinar el olfato de la organización frente a la inseguridad, la formalización de la aplicación de las buenas prácticas de seguridad y la responsabilidad de cada persona frente a la información y el compromiso del área de seguridad para facilitar su buen uso en el contexto de los procesos de negocio.

Resiliencia organizacional

La convergencia de la seguridad, según lo define el documento, *Security Convergence* and ERM[1]., realizado por la *Alliance for Enterprise Security Risk Management*, es la integración, de manera formal, colaborativa y estratégica, de los recursos de seguridad de una organización, con el fin de entregar beneficios empresariales frente a la mitigación de riesgos, mejoramiento de la efectividad operacional, eficiencia y disminución de costos.

Esta definición marca la ruta que las organizaciones actuales exigen frente a un entorno agreste y lleno de desafíos que atentan contra la continuidad de las operaciones de las empresas. En razón con lo anterior, se advierte la presencia de una nueva característica requerida no sólo a nivel del sistema de gestión de seguridad, sino como parte inherente del sistema de control interno corporativo que se denomina resiliencia.

“El vocablo resiliencia tiene su origen en el idioma latín, en el término

resilio, que significa volver atrás, volver de un salto, resaltar, rebotar. El término fue adaptado a las ciencias sociales para caracterizar aquellas personas que a pesar de nacer y vivir en situaciones de alto riesgo, se desarrollan psicológicamente sanos y exitosos" (KOTLIARENCO, CÁCERES y FONTENCILLA 1997, pág.13)

Contextualizando esta definición en el escenario corporativo podríamos decir que es la característica de las organizaciones que a pesar de estar sometidas a incidentes y materialización de riesgos, son capaces de continuar operando y manteniendo la dinámica de sus negocios, de tal forma que son capaces de recomponerse a su estado original, aprender de cada una de ésta situaciones y fortalecer su gestión estratégica en su entorno competitivo.

Si lo anterior es cierto, ya no es la administración o la gestión de seguridad de la información la que tiene mantener la confiabilidad de la información en los procesos de negocio, sino el gobierno de la seguridad de la información (BROTBY 2009) es la nueva instancia que esta llamada a concretar en cada momento y artefacto cultural, una práctica de resiliencia de las operaciones, que no es otra cosa que el reconocimiento de la crisis como la manera de promover la adaptación permanente de la organización a la evolución de los riesgos.

Reflexiones finales

Observar la evolución de la inseguridad informática y monitorizar los resultados de sus acciones, es un ejercicio táctico y estratégico que el responsable de la seguridad de la información debe desarrollar como parte inherente de su función de negocio. El no poder detallar patrones emergentes o vectores de ataques novedosos, lo deja en una posición poco ventajosa que necesariamente impactará su gestión de seguridad de la información.

Los directores de seguridad de la información o llamados en la literatura *Chief Information Security Officers* – CISO, deben mantener una posición vigilante que les permita incorporar en su gestión de manera proactiva elementos como la cultura de seguridad, las acciones de cumplimiento, la tendencias en computación móvil, los ataques de día cero entre otras actividades, con el fin de avanzar tanto como los atacantes nos logran sorprender.

Sin un entendimiento y mirada crítica a los patrones de tendencias en seguridad de la información, sin una adecuada interiorización de una cultura de seguridad y sin un referente particular que guíe la práctica de la gestión de la seguridad, las organizaciones estarán avocadas a ser blanco permanente de las inseguridad, de los incidentes y las implicaciones legales.

Cuando logramos articular en la gestión de seguridad, un conocimiento responsable de las fallas, una particular motivación al logro, un alto convencimiento y mercadeo de la seguridad y sobre manera, la confianza e integridad de nuestras acciones, las prácticas de protección de la información dejan de ser algo que se hace por cumplir y se transforman en una ventaja estratégica que se desea fortalecer.

Detallar la evolución y la monitorización de la seguridad de la información, debe ser un hábito corporativo, una responsabilidad de cada persona que participa en ella y el compromiso del área de seguridad. Una estrategia práctica y real para afianzar la gestión y el aseguramiento de la información que permita entender las motivaciones de la gerencia y así, generar valor para sus clientes.

Notas de pie de página

[1.] *Documento disponible en: http://www.aesrm.org/files/Convergence_SecProf_View_5Mar09_Research.pdf (Consultado: 25-05-2009)*

Referencias

[1] BROTBY, K. (2009) Information security governance. A practical development and implementation approach. John Wiley & Sons.

[2] CURPHEY, M. y ARAUJO, R. (2006) Web application security assessment tools. IEEE Security & Privacy. July/August.

[3] ETGES, R. y McNEIL, K. (2006) Understanding data classification based on business and security requirements. ISACA Information Systems Control Journal. No.5.

[4] KOTLIARENCO, M., CÁCERES, I. y FONTENCILLA, M. (1997) Estado del arte en Resiliencia. Organización Panamericana de la Salud. CEANIM – Centro de Estudios y Atención del Niño y la Mujer. Disponible en: http://www.paho.org/Spanish/HPP/HPF/ADOL/Resil6x9.pdf (Consultado: 25-05-2009)

[5] LACEY, D. (2009) Managing the human factor in information security. John Wiley & Sons.

[6] McAFEE, A. (2006) Mastering the three worlds of information technology. Harvard Business Review. November.

[7] SCHNEIER, B. (2004) Security and compliance. IEEE Security & Privacy. July/August.

SPANG, S. (2009) Five trends that will shape business technology in 2009. Mckinsey Quarterly. No.15. Spring.

[8] TANEY Jr., F. y COSTELLO, T. (2006) Securing the whole enterprise: Business and legal issues. IEEE IT Professional. January/February.

[9] WESTNEY, E. (2008) Three perspectives on organizational change. Leading Change in Complex Organization. MIT Sloan School of Management. Executive Program. June

[10] WILBANKS, L. (2008) Need to share vs. need to assure. IEEE IT Professional. May/June.

Sobre el Autor:
Jeimy J. Cano, Ph.D, CFE. *Miembro investigador del Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática (GECTI) de la Facultad de Derecho y Profesor Distinguido de la misma Facultad, Universidad de los Andes. Colombia. Ingeniero de Sistemas y Computación, Universidad de los Andes. Magíster en Ingeniería de Sistemas y Computación, Universidad de los Andes. Ph.D in Business Administration, Newport University. Profesional certificado como Certified Fraud Examiner (CFE) por la Association of Certified Fraud Examiners. Presidente de ACIS durante el periodo 2005-2007 jjcano@yahoo.com*