contenido

Publicación de la Asociación Colombiana de
Ingenieros de Sistemas (ACIS)
Resolución No. 003983 del
Ministerio de Gobierno
Tarifa Postal Reducida No. 2010-186.4-72
Servicios Postales Nacionales
ISSN 0120-5919
Apartado Aéreo No. 94334
Bogotá D.C., Colombia

Abril-Junio 2011
Calle 93 No. 13-32 Of. 102
Tels.: 616 1407 – 616 1409
A.A. 94334
Bogotá D.C.
www.acis.org.co

Software Security & Integrity

Ushiro Security, Llevamos la Seguridad de la Información al siguiente nivel. Con un enfoque preventivo, pragmático y un completo portafolio de soluciones ofrecemos a nuestros clientes alinear las prioridades del negocio con las áreas de tecnología. Eliminamos todo riesgo que puede impactar en el nivel de servicio, excelencia operacional, satisfacción del cliente y el cumplimiento de regulaciones legales.

Damos visibilidad y control sobre desarrollos internos, externos y open-source, cambiando la incertidumbre por confiabilidad y un alto nivel de servicio del Software.

Prevención y Detección Temprana de Defectos	Control de Políticas de Calidad del Software	Desarrollo de Software Seguro - Consultoría	Desarrollo de Software Seguro - Entrenamiento	Análisis Estático, Dinámico y Arquitectura

coverity

armorize
Secure Your Web Application

VERACODE

Contamos con una amplia experiencia y base de conocimiento implementando las soluciones líderes del mercado de Integridad del Software. Gracias a Coverity detectamos tempranamente defectos graves que ponen riesgo el Software.

Prevenir las vulnerabilidades de aplicaciones Web ha sido nuestro objetivo, junto a Armorize la prevención y remediación de Vulnerabilidades en Aplicaciones Web se logra de manera efectiva y eficaz.

Por que detectar las vulnerabilidades donde se producen es la clave. Con las soluciones de VeraCode el detectar vulnerabilidades analizando un binario o sitio Web (Penetration Test) se hace fácil y rentable.

www.ushiro-sec.com 6386154 contacto@ushiro-sec.com

Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global

Jeimy J. Cano

Los eventos recientes sobre fuga de información, las noticias de atacantes informáticos doblegando protocolos y tecnologías de seguridad, las fallas de seguridad que se han presentado tanto en el sector público como en el sector privado, son argumentos suficientes para evidenciar que estamos en un nuevo escenario de riesgos y amenazas, donde la información se convierte en un arma estratégica y táctica, que cuestiona la gobernabilidad de una organización o la de una nación. (CANO, J. 2008).

En este contexto, los ejercicios de riesgos y controles propios de las empresas, para establecer y analizar los activos de información críticos, han dejado de ser *"algo que hacen los de seguridad"* para transformarse día con día en una disciplina que adopta la organización, para hacer de su gestión de la información una ventaja clave y competitiva frente a su entorno de negocio. Por tanto, la figura opcional de la seguridad de la información, comienza a desvanecerse y a tomar una relevancia estratégica, ahora en un escenario donde la información, es la *"moneda fundamental"* para generar, proponer y desarrollar posiciones privilegiadas de personas, empresas y naciones.

Cuando elevamos esta reflexión a nivel de Estados y países, encontramos múltiples vistas para comprender los riesgos y amenazas frente a la información y sus impactos, que generan confusión y desconfianza, generalmente aprovechadas por los escépticos, para reparar en comentarios poco constructivos, que tratan de limitar la importancia de estos temas. Sin embargo, los hechos y eventos que se han presentado, mantienen la atención de gobiernos sobre estos peligros, que aunque escondidos en el tejido de las noticias cotidianas, son actores claves de las relaciones internacionales y la capacidad de reacción de un Estado. (McAFEE 2009).

Reconociendo al enemigo digital: Ciberdefensa

Una primera estrategia que adoptan los Estados cuando reconocen *"al nuevo enemigo"* en el contexto de una sociedad de la información y el conocimiento, es reconocer que cuenta con infraestructura de información crítica, requerida para mantener la operación y gobernabilidad de la nación. Siguiendo la directiva presidencial No.13010, firmada por el presidente norteamericano Bill Clinton en 1998 (US CONGRESS 1998), se definen ocho sectores críticos cuyos servicios son vitales para el funcionamiento de la nación, y la incapacidad de operación o destrucción tendría un impacto directo en la defensa o en la seguridad económica de los Estados Unidos. Tales sectores son: energía eléctrica, producción, almacenamiento y suministro de gas y petróleo, telecomunicaciones, bancos y finanzas, suministro de agua, transporte, servicios de emergencia y operaciones gubernamentales (mínimas requeridas para atender al público).

Así las cosas, un ataque masivo y coordinado a alguno o varios de estos sectores establece una condición importante y crítica para una nación, pues se pone en juego la estabilidad de lamisma y la confianza de la ciudadanía en su gobierno para enfrentarse a estas amenazas. En este sentido, el concepto de guerra tradicional, se transforma para darle paso a una nueva función del Estado frente a la defensa de su soberanía en el espacio digital y la protección de los derechos de sus ciberciudadanos, ante las amenazas emergentes en el escenario de una vida más digital y gobernada por la información.

En consecuencia, se acuña el término de **ciberdefensa** como esa nueva connotación sistémica y sistemática que deben desarrollar los gobiernos, para comprender ahora sus responsabilidades de Estado, en el contexto de un ciudadano y las fronteras nacionales electrónicas o digitales. Un concepto estratégico de los gobiernos que requiere la comprensión de variables como, las vulnerabilidades en la infraestructura crítica de una nación; las garantías y derechos de los ciudadanos en el mundo online; la renovación de la administración de justicia en el entorno digital; y, la evolución de la inseguridad de la información en el contexto tecnológico y operacional.

En tal sentido, las reflexiones y decisiones sobre la seguridad nacional, tienen una renovada connotación, para atender ahora un enemigo móvil, cambiante y evolucionado, que se mueve tanto en las infraestructuras críticas como fuera de ellas; que sabe lo reactivo de las empresas y gobiernos; y que, a pesar de que pueda ser identificado en sus ataques, es poco creíble probar que existió.

La defensa nacional, como noción acuñada por las fuerzas militares de un país, requiere ser analizada y repensada en el contexto del *"nuevo rostro de la guerra"*, de una confrontación que enfrenta lo mejor de los entrenados en el arte de la inseguridad de la información, con lo mejor de los entrenados para controlar y mantener la paz de una nación. Por tanto, animar una revisión de las estrategias de seguridad nacional ante posibles y factibles escenarios de confrontación tecnológica y de guerra de la información, prepara a los Estados para defender su

gobernabilidad y asegurar su resiliencia en condiciones de falla parcial o total.

A la fechas muchos Estados (generalmente de países desarrollados) han tomado acciones concretas en el reto de la ciberdefensa, encontrando en sus ciudadanos los primeros y más importantes aliados para sus estrategias de protección de la nación en el contexto digital. Dichos Estados comprenden que es, desde el ciudadano y su experiencia en el uso de las tecnologías de información y comunicaciones, donde pueden fortalecer el perímetro extendido de seguridad nacional digital. Conocedores de que es poroso y poco confiable, saben que allí encuentran su mejor carta para hacer realidad su visión de defensa de la nación en un mundo interconectado. (CANO, J. 2008b)

Detallando las prácticas de aseguramiento: ciberseguridad

Para darle vida a esta visión de la defensa nacional digital, se requieren elementos específicos que materialicen ese querer en acciones detalladas, que aplicadas en las tecnologías de información e interiorizadas en los hábitos de los ciudadanos, puedan hacer evidente esa nueva propiedad emergente, denominada seguridad nacional digital, que genera confianza, respeto y confiabilidad en las iniciativas del gobierno ante la realidad de la creciente dinámica informática y de las telecomunicaciones.

Considerando lo anterior, es evidente que los gobiernos no pueden hacer realidad su nueva visión de la defensa, sin una estrategia concreta de prácticas de seguridad de la información, como base fundamental de su visión de seguridad nacional, donde cada uno de los individuos reconozcan en la información un activo fundamental que articula todas las infraestructuras críticas de la nación, y que hace realidad el sueño de una sociedad "informada".

Así las cosas, el concepto de **ciberseguridad**, como realidad complementaria de la ciberdefensa, materializa el concepto de defensa nacional digital, en un conjunto de variables claves, acertadamente definidas por la ITU -International Telecommunication Union-, en las cuales son necesarias el desarrollo de prácticas primordiales para darle sentido y real dimensión a la seguridad de una nación, en el contexto de una realidad digital y de información instantánea.

La ITU, entendiendo que la problemática de la ciberseguridad requiere un esfuerzo colectivo y coordinado entre los diferentes países, establece cinco elementos fundamentales para desarrollar una estrategia de ciberseguridad, acorde con la realidad de cada una de las naciones: desarrollo de un marco legal para la acción, desarrollo y aplicación de medidas técnicas y procedimentales, diseño y aplicación de estructuras organizacionales requeridas, desarrollo y aplicación de una cultura de ciberseguridad y la cooperación internacional. (ITU 2010)

Cada una de las variables establecidas por la ITU, no buscan otra cosa que comprender los riesgos propios de una sociedad de la información digital y en constante movimiento, que considere los aspectos normativos, las tecnologías de seguridad de la información, la organización de la seguridad de la información necesaria

para operar, la cultura de seguridad de la información y la cooperación entre países, como fuente de la armonización de visión de la ciberseguridad en el planeta.

Reflexiones finales

De acuerdo con lo planteado, cuando hablamos de ciberseguridad, necesariamente debemos considerar las acciones básicas que desarrolla una nación para proteger de manera coherente, sistemática y sistémica los activos de información crítica, distribuidos en toda su infraestructura y cómo ellos impactan la operación del Estado.

De la mano con los conceptos de ciberdefensa y ciberseguridad, se han venido desarrollando reflexiones académicas y de la industria, relacionadas con ciberterrorismo y cibercrimen (CANO, J. 2008), dos amenazas emergentes en una sociedad digital, las cuales han comenzado a inquietar a los ciudadanos, quienes hoy por hoy se sienten expuestos frente a la materialización de las mismas y sus efectos reales sobre la confianza en el Estado y sus instituciones.

Si bien la ciberdefensa como la ciberseguridad, son temas de estudio e investigación actual, tanto en la industria, la academia y el gobierno, es claro que requieren atención inmediata con acciones definidas que permitan comunicar a los potenciales agresores, que estamos preparados para enfrentar el reto de un ataque informático coordinado, para hacer respetar nuestra soberanía nacional digital.

Referencias

[1] ITU (2010) Global cybersecurity agenda. Disponible en: http://www.itu.int/osg/csd/cybersecurity/gca/new-gca-brochure.pdf

[2] US CONGRESS (1998) PRESIDENTIAL DECISION DIRECTIVE/NSC-63. Disponible en: http://www.fas.org/irp/offdocs/pdd/pdd-63.htm

[3] CANO, J. (2008) Cibercrimen y ciberterrorismo. Dos amenazas emergentes. [4]ISACA Information Control and Audit Journal. Vol 6. Disponible en: http://www.isaca.org/Journal/Past-Issues/2008/Volume-6/Pages/JOnline-Cibercrimen-y-Ciberterrorismo-Dos-Amenazas-Emergentes.aspx

[4] CANO, J. (2008b) La guerra fría electrónica y la inseguridad de la información. Publicación en Blog. Disponible en: http://www.eltiempo.com/participacion/blogs/default/un_articulo.php?id_blog=3516456&id_recurso=450012245&random=4197

[5] McAFEE (2009) Virtual Criminology Report 2009. Virtually Here: The age of cyber warfare. Disponible en: http://www.mcafee.com/us/resources/reports/rp-virtual-criminology-report-2009.pdf

Jeimy J. Cano. *Ph.D, CFE. Ingeniero y Magíster en Ingeniería de Sistemas y Computación de la Universidad de los Andes. Ph.D en Administración de Negocios de Newport University, CA. USA. Executive Certificate in Leadership and Management del MIT Sloan School of Management. Profesor Distinguido y miembro del Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática de la Facultad de Derecho de la Universidad de los Andes. Examinador Certificado de Fraude – CFE por la ACFE y Cobit Foundation Certificate por ISACA.*

Los CISO´s opinan

La seguridad de la información, en las voces autorizadas de quienes tienen esa gran responsabilidad.

La revista Sistemas se ocupó de indagar sobre los aspectos más relevantes alrededor de la seguridad de la información. Asuntos tales como los retos para mitigar los riesgos o las acciones emprendidas para que los directivos de las organizaciones contemplen este activo en sus agendas, entre otros, fueron abordados por Javier Díaz Evans, director de Seguridad de la Información en ATH S.A.; Andrés Ricardo Almanza Junco, coordinador de Seguridad de la Información en la Cámara de Comercio de Bogotá; Francisco Pacheco Alfonso, director de Seguridad de la Información en Deceval S.A.; y, Carlos Alberto Zambrano Smith, director Seguridad de la Información para América Latina en la Organización Terpel S.A.

Las preguntas para todos

1. En un entorno gobernado por la movilidad, negocios en línea y una mayor demanda de servicios, ¿cuáles son los retos más importantes, desde el punto de vista de seguridad de la información, que se deben atender para balancear: la mitigación de los riesgos frente a la información y la agilidad que demanda el negocio?

2. En un escenario de tecnologías convergentes, donde lo físico y lo lógico son cada vez más parte de una misma vista, ¿cuáles retos advierten los CISO frente al gobierno de la seguridad de la información a nivel empresarial?

3. No hay duda de que día tras día, tenemos más clientes empoderados y llenos de requerimientos para realizar en forma más rápida y más simple sus actividades, y la seguridad no es una de sus prioridades. En este contexto, ¿cuáles estrategias se deben adelantar para integrar la distinción de seguridad de la información, en esta dinámica empresarial y global?

4. Con las recientes noticias sobre espionaje informático y fugas de información es evidente que la información es un activo crítico representado con números importantes en el P&G de una empresa. Bajo tal premisa, ¿qué acciones se vienen desarrollando en su empresa para incluir este activo en las agendas de los directivos?

5. Ciberseguridad y ciberdefensa son dos conceptos emergentes en la actualidad. ¿Cuál debería ser la posición del CISO frente a esta realidad? ¿Qué recomendaciones debe ofrecer a la organización en estos temas?

Javier Díaz Evans
Director de Seguridad de la Información
ATH S.A.

Revista Sistemas: En un entorno gobernado por la movilidad, negocios en línea y una mayor demanda de servicios, ¿cuáles son los retos más importantes, desde el punto de vista de seguridad de la información, que se deben atender para balancear: la mitigación de los riesgos frente a la información y la agilidad que demanda el negocio?

Javier Díaz Evans: Desde hace algunos años hemos orientado esfuerzos en incluir dentro de nuestra arquitectura de seguridad la estrategia de eliminación de las fronteras. Esta nueva visión de la seguridad cambia la mentalidad de los administradores de seguridad, orientados a proteger la información con barreras y paredes como si fuera un bien tangible. En la actualidad, la arquitectura de seguridad debe extenderse a la protección de dispositivos y de datos, controlar no sólo por fuentes y destinos, sino por comportamiento, usuarios y sensibilidad de los datos.

RS: En un escenario de tecnologías convergentes, donde lo físico y lo lógico son cada vez más parte de una misma vista, ¿cuáles retos advierten los CISO frente al gobierno de la seguridad de la información a nivel empresarial?

JDE: El Gobierno de Seguridad tiene unos objetivos claramente definidos, entre ellos encontramos: alineación estratégica, gestión de riesgos, administración de recursos, entrega de valor y medición de desempeño.

Dentro de los grandes retos que encontramos están la unificación de metodologías de riesgo, para garantizar que se orienten los esfuerzos en la gestión de los más sensibles de la organización, sean de seguridad lógica, física, riesgo operativo o auditorías internas. Esa convergencia de modelos de riesgos debe garantizar la unificación de conceptos, la estandarización de medidas y el reporte único de los diferentes hallazgos identificados.

RS: No hay duda de que día tras día, tenemos más clientes empoderados y llenos de requerimientos para realizar en forma más rápida y más simple sus actividades, y la seguridad no es una de sus prioridades. En este contexto, ¿cuáles estrategias se deben adelantar para integrar la distinción de seguridad de la información, en esta dinámica empresarial y global?

JDE: El desarrollo de aplicaciones debe tener un equilibrio entre facilidad de uso, funcionalidad y seguridad. Es necesario reducir al máximo los controles que son responsabilidad del usuario, debido a que son inefectivos. Las estrategias están orientadas a incluir la seguridad de la información en el ciclo de vida de los sistemas (no le enseñe seguridad a su desarrollador), y la seguridad en el ambiente de usuario final.

RS: Con las recientes noticias sobre espionaje informático y fugas de información es evidente que la información es un activo crítico representado con números importantes en el P&G de una empresa. Bajo tal premisa, ¿qué acciones se vienen desarrollando en su empresa para incluir este activo en las agendas de los directivos?

JDE: El sector financiero ha comprendido bien que el dinero dejo de ser un tema físico, en la actualidad las grandes sumas de dinero son datos incluidos en los sistemas core de los bancos, cualquier problema de integridad puede eliminar todo el dinero de los bancos o triplicarlo en un segundo. Los presidentes, comités directivos y las juntas directivas tienen claro este tipo de riesgos y la necesidad de gestionarlos.

RS: Ciberseguridad y ciberdefensa son dos conceptos emergentes en la actualidad. ¿Cuál debería ser la posición del CISO frente a esta realidad? ¿Qué recomendaciones debe ofrecer a la organización en estos temas?

JDE: La seguridad no es una ciencia exacta, lo que puede ser bueno para algunos puede no ser efectivo para otros; el "Ecosistema de Seguridad" unir a clientes, proveedores, expertos para aportar al modelo es fundamental. Debido a esto es necesario establecer una estrategia de inteligencia de seguridad, para garantizar que se responda en forma oportuna a las nuevas amenazas y vulnerabilidades que pueden impactar a la organización. Para esto comparto algunas recomendaciones que pueden ayudar a apalancar dicho objetivo:

- Sistemas de correlación de eventos (SIEM).
- Definición de planes e instructivos de respuesta ante eventos de seguridad.
- Establecimiento de equipo de atención de emergencias.
- Establecimiento del Ecosistema de Seguridad.

Andrés Ricardo Almanza Junco
Coordinador de Seguridad
de la Información
Cámara de Comercio de Bogotá

Revista Sistemas: En un entorno gobernado por la movilidad, negocios en línea y una mayor demanda de servicios, ¿cuáles son los retos más importantes, desde el punto de vista de seguridad de la información, que se deben atender para balancear: la mitigación de los riesgos frente a la información y la agilidad que demanda el negocio?

Andrés Ricardo Almanza Junco: En este contexto es necesario tener claro

que el balance de estos mundos está dado por el uso adecuado de la tecnología; por una participación cerrada en la construcción de aplicaciones seguras; además de reforzar el entrenamiento a los usuarios finales, para mantener de manera consistente un ambiente adecuado de seguridad en los servicios prestados. De igual manera debe haber como premisa máxima un compromiso de la organización, amparado en una buena estrategia de seguridad de la información, que respalde las iniciativas tácticas y operacionales en los temas que conciernen a la prestación de servicios de manera virtual.

RS: En un escenario de tecnologías convergentes, donde lo físico y lo lógico son cada vez más parte de una misma vista, ¿cuáles retos advierten los CISO frente al gobierno de la seguridad de la información a nivel empresarial?

ARAJ: En primera instancia creo que debemos traspasar las barreras de ver a los dos mundos por separado. Las organizaciones deben asumir el papel de poder integrar a las personas responsables de los dos mundos; el gran reto está en que el responsable de la seguridad física, no se sienta aislado en el momento de pensar en la protección de la información ni sienta que al integrar las dos áreas el motivo sea recortar personal, el presupuesto o algo de este estilo. Por el contrario, es necesario acercarlo haciéndole ver importancia de su labor dentro del marco de gobierno de la seguridad de la organización. Reto importante es mostrar los beneficios que las tecnologías de protección física les pueden ofrecer a estas unidades de apoyo corporativo, y su valor para maximizar la prestación del servicio requerido del mundo de seguridad física. Es inminente vender la necesidad de que no sólo los servicios de vigilancia a través de personas son las únicas alternativas posibles y disponibles para garantizar la seguridad física. Hay que velar porque la organización entienda la importancia de proteger la información y que dentro de esta arquitectura para blindarla, un anillo más de este modelo es la seguridad física como elemento de vital importancia en la protección.

RS: No hay duda de que día tras día, tenemos más clientes empoderados y llenos de requerimientos para realizar en forma más rápida y más simple sus actividades, y la seguridad no es una de sus prioridades. En este contexto, ¿cuáles estrategias se deben adelantar para integrar la distinción de seguridad de la información, en esta dinámica empresarial y global?

ARAJ: En primera instancia, creo que la estructuración de los procesos de seguridad puede dar un respaldo sólido a la necesidad de tener presente la seguridad en la creación de servicios de negocio. La construcción de cultura corporativa en los temas de protección de la información, es otra de las estrategias que pueden servir a la hora de crear modelos de negocio, en los cuales la seguridad de la información esté involucrada. La presencia de entes regulatorios externos, si bien ejerce un carácter obligante, también ayuda como un garante no interno a que la seguridad de la información esté embebida como parte natural de la operación del negocio.

RS: Con las recientes noticias sobre espionaje informático y fugas de información es evidente que la información es un activo crítico representado con números importantes en el P&G de una empresa. Bajo tal premisa, ¿qué acciones se vienen desarrollando en su empresa para incluir este activo en las agendas de los directivos?

ARAJ: Es de vital importancia poseer claras formas que permitan identificar, valorar, clasificar, y catalogar los activos de la información de la organización. Por lo tanto, se deben estructurar los debidos procesos que permitan realizar estas labores. Así mismo, es de carácter obligatorio en el momento de estructurar estos procesos, hacerle ver a la organización, a través de los niveles directivos, que no son las áreas tecnológicas ni las de seguridad de la información, las dueñas de los activos. En consecuencia, estas responsabilidades deben ser asumidas por los verdaderos dueños de los negocios, que en últimas dada su condición, son los que definen las reglas sobre cómo proteger la información. Los responsables de la seguridad de la información seremos los garantes de gestionar el proceso, y las áreas de tecnología serán las custodias de una serie de medidas tecnológicas en pro de proteger los activos de información definidos.

RS: Ciberseguridad y ciberdefensa son dos conceptos emergentes en la actualidad. ¿Cuál debería ser la posición del CISO frente a esta realidad? ¿Qué recomendaciones debe ofrecer a la organización en estos temas?

ARAJ: Hay que entender que nuestro perímetro es mucho más extenso. Es necesario que los CISO's tengamos una posición vigilante, atenta, decidida, por conocer más el mundo en el que la información de la organización se presta. Es necesario que nos introduzcamos en el mundo del negocio, desde la perspectiva de la seguridad e imprimir esa necesidad al mismo. Así mismo, se requiere que nosotros seamos los que pensemos en la forma en cómo consolidar un posible ataque, y de esa manera diseñar nuestras estrategias de protección, Es necesario un entrenamiento continuo acerca de las nuevas tecnologías de información, una nube que agobia cada vez más a las organizaciones, una movilidad que rompe los paradigmas, una necesidad cada vez mayor de prestar mayores servicios de manera eficiente y eficaz. Una obligación ineludible para mantenerse en una economía cambiante. Un sinnúmero de variables adicionales que hacen del CISO una persona multifacética, con una orientación a entender dos mundos, la tecnología y el negocio, con unas interfaces que claramente deben responder a lo que la organización requiere. Atrás deben quedar las visiones técnicas unitarias que muestran a la seguridad de la información como un conjunto de componentes tecnológicos; atrás debe quedar una postura simplista de que la tecnología es suficiente; debe estar en la bandera poseer una capacidad de analizar un negocio, entenderlo y determinar cuáles necesidades se tienen frente a lo que la organización quiere, lo que los clientes esperan, lo que los enemigos realizarán, y lo que la seguridad podrá aportar para disminuir esas fuentes de riesgos que pueden verse materializadas dentro de la organización para afectarla.

Francisco Pacheco Alfonso
Director de Seguridad
de la Información
Deceval S.A.

Revista Sistemas: En un entorno gobernado por la movilidad, negocios en línea y una mayor demanda de servicios, ¿cuáles son los retos más importantes, desde el punto de vista de seguridad de la información, que se deben atender para balancear: la mitigación de los riesgos frente a la información y la agilidad que demanda el negocio?

Francisco Pacheco Alfonso: Un riesgo que origina la movilidad y los negocios en línea es la repudiación de los acuerdos que a través de este tipo de canales se hagan. Otro riesgo potencial que se desprende del anterior, es desde que se decide crear y/o trasladar los servicios y productos a la nube, no conceptuar y generar protocolos y políticas de trazabilidad, registro y copia (back-up) que permitan un establecimiento fácil, además de una adecuada cadena de custodia a los elementos o condiciones probatorios que aseguren la no repudiación. Como complemento a los anteriores, está el riesgo de cumplimiento legal y regulatorio que gira alrededor de la movilidad; con un marco legal no claro ni aterrizado a las condiciones económicas y tecnológicas de Colombia y su integración con el mundo. Finalmente, está el riesgo relacionado con nuestra cultura. Los retos que genera la minimización de los riesgos anteriormente expuestos contempla encontrar elementos tecnológicos fuertes que cumplan con las condiciones regulatorias de carácter nacional, las cuales están contaminadas, se prestan a múltiples interpretaciones y, de cierta manera, no permiten, restringen o hacen más costosa la internacionalización de esos productos y servicios.

RS: En un escenario de tecnologías convergentes, donde lo físico y lo lógico son cada vez más parte de una misma vista, ¿cuáles retos advierten los CISO frente al gobierno de la seguridad de la información a nivel empresarial?

FPA: Indudablemente se debe tender a la convergencia de las seguridades para gobernar las tres dimensiones: Seguridad de la Información, Seguridad Física y Seguridad Ambiental. El BS7799-2 de hecho lo prevé, tiene la Seguridad Física y la Seguridad Ambiental inmersas en uno de sus pilares (Bs-9 Seguridad Física y Del Entorno), quedando un faltante por complementar, lo cual podrá extractarse en lo que aplique, según el tipo de industria, de la

ISO14000. El liderazgo de un experto en seguridad de la información, un experto en seguridad física o un experto en seguridad ambiental, deberá ser definido de acuerdo con la clase de industria, teniendo en cuenta que cada tipo de seguridad no debe perder su foco y todas en su conjunto deberán ser gobernadas por un mismo enfoque integral de riesgo. Finalmente y para que esta convergencia sea óptima y perdurable en la empresa, debe estar acompañada de elementos de gobierno, riesgo y cumplimiento, tal cual lo prevé y visualiza el BS-7799-2

RS: No hay duda de que día tras día, tenemos más clientes empoderados y llenos de requerimientos para realizar

en forma más rápida y más simple sus actividades, y la seguridad no es una de sus prioridades. En este contexto, ¿cuáles estrategias se deben adelantar para integrar la distinción de seguridad de la información, en esta dinámica empresarial y global?

FPA: Lo respondo de manera simple. Nosotros como responsables de la seguridad de la información tenemos la obligación de identificar, enterar y aclarar los riesgos potenciales, derivados de una decisión corporativa como lo es la de no asumir la seguridad de la información como prioridad. Con base en este ejercicio la empresa decidirá si aumenta o no su apetito al riesgo; por ende deberá eventualmente asumirlos, aceptarlos e informar a su junta directiva las condiciones del nuevo panorama de riesgos. La cultura de riesgo debe ser una condición de manejo universal para la gestión de la empresa.

RS: Con las recientes noticias sobre espionaje informático y fugas de información es evidente que la información es un activo crítico representado con números importantes en el P&G de una empresa. Bajo tal premisa, ¿qué acciones se vienen desarrollando en su empresa para incluir este activo en las agendas de los directivos?

FPA: Netamente gestión de riesgos e inventario y clasificación de los activos de información en niveles altos.

RS: Ciberseguridad y ciberdefensa son dos conceptos emergentes en la actualidad. ¿Cuál debería ser la posición del CISO frente a esta realidad? ¿Qué recomendaciones debe ofrecer a la organización en estos temas?

FPA: Las empresas sólo deben llevar a la nube lo que las hace comunes con su competencia.

Carlos Alberto Zambrano Smith

Director Seguridad de la Información para América Latina
Organización Terpel S.A.

Revista Sistemas: En un entorno gobernado por la movilidad, negocios en línea y una mayor demanda de servicios, ¿cuáles son los retos más importantes, desde el punto de vista de seguridad de la información, que se deben atender para balancear: la mitigación de los riesgos frente a la información y la agilidad que demanda el negocio?

Carlos Alberto Zambrano Smith: La seguridad de la información debe ser una marco cambiante que ayude a balancear la operación de la empresa y la mitigación del riesgo, con el objetivo de ser competitivo dentro del mercado, al considerar que la movilidad, los negocios en línea, así como los servicios que se deben prestar no pueden verse como un obstáculo, sino como una oportunidad de afianzar la madurez de la seguridad que complementa de manera directa la prestación del servicio, en la protección de la información de la compañía y del cliente externo. Al combinar el equilibrio de la organización y el cliente externo, es posible obtener un resultado de posicionamiento y de imagen en la integridad de los datos, incalculable en sus valores.

El principal reto de la seguridad de la información es el desafío ante estas nuevas tecnologías de alto consumo y demanda para proteger la información, cuando por su naturaleza tecnológica interactúa de manera ilimitada con el mundo externo. Este desafío es resuelto a través de la transformación (cultura de seguridad de la información); que seguridad lidere en el interior de la organización y que, a su vez, defina lineamientos claros de las responsabilidades y limitaciones entre el negocio y el cliente externo, llámese demanda de servicios, prestación, servicios en línea etc. La transformación ayuda a generar un impacto significativo en las personas, las empresas, el gobierno y la sociedad. Una vez alcanzada la transformación se deberá complementar con lineamientos y políticas, encaminadas a controlar la prestación del servicio ante actividades que afecten la integridad, confidencialidad y disponibilidad.

RS: En un escenario de tecnologías convergentes, donde lo físico y lo lógico son cada vez más parte de una misma vista, ¿cuáles retos advierten los CISO frente al gobierno de la seguridad de la información a nivel empresarial?

CAZS: Las tecnologías convergentes tales como la geolocalización (Ip fijas, Wifi, Gps), nanotecnologías, Inteligencias (control de accesos, abusos de sistemas, calidad de servicios, aplicaciones automáticas), entre otras, conforman un espacio físico y lógico, siendo este último de mayor crecimiento y difícil de identificar la frontera entre ellos.

El principal reto es el control de lo lógico y por ende al definir los lineamientos, los CISO deben enmarcar como ente importante la CONCIENTIZACIÓN y el MONITOREO permanentes de los sistemas de información que transitan en ambas vías, en las tecnologías convergentes y las plataformas que los sostienen.

Uno de los escenarios que ayudan a definir la integridad de la información de la parte lógica es la correlación de eventos, en donde se expresan los estados, las condiciones, las acciones y plazos de los datos que son calculados de manera virtual. Por ende el MONITOREO es crucial y es la visibilidad de los CISO en su gobierno. Cabe resaltar que las inversiones necesarias para la trazabilidad de las mismas, deben estar bajo un programa de CONCIENTIZACIÓN desde la cúspide de la organización, hasta el nivel inferior.

Las tecnologías convergentes y cualquier espacio deben responder a la estrategia del negocio y, a su vez, definir los procesos que la soportan con el uso de los sistemas de información. Es importante el desarrollo y la implementación de la matriz de riesgo, que a su vez se convierte en el insumo para el MONITOREO.

RS: No hay duda de que día tras día, tenemos más clientes empoderados y llenos de requerimientos para realizar en forma más rápida y más simple sus actividades, y la seguridad no es una de sus prioridades. En este contexto, ¿cuáles estrategias se deben adelantar para integrar la distinción de seguridad de la información, en esta dinámica empresarial y global?

GAZS: Por experiencia propia a los clientes se les debe educar a través de

los intereses propios que afectan la operación y su gestión, ante la pérdida de la disponibilidad o la integridad del sistema de información. Lo anterior se logra culturizando a los clientes mediante programas permanentes de comunicaciones y talleres sobre casos reales de su información y el impacto del mismo, ante un riesgo materializado. La estrategia que siempre aplico es el dolor de la pérdida de información confidencial y su trazabilidad por omisión del debido proceso que el cliente realiza, esto se hace por medio de la concientización. La estrategia de la concientización se desarrolla como proyectos y debe estar siempre como una constante en los planes de la seguridad de la información anual, y debe ser implementada en todos los rincones de la organización y las responsabilidades de cada cliente interno con los externos. Al aplicar educando para educar se logra la madurez y, a través de esto se llega a un equilibrio entre seguridad y el requerimiento de las necesidades del negocio.

RS: Con las recientes noticias sobre espionaje informático y fugas de información es evidente que la información es un activo crítico representado con números importantes en el P&G de una empresa. Bajo tal premisa, ¿qué acciones se vienen desarrollando en su empresa para incluir este activo en las agendas de los directivos?

CAZS: Unos de los titulares que nos hace pensar fue lo realizado por una firma internacional sobre las tendencias de espionaje y fuga de información, en la cual Colombia es subcampeón mundial del fraude tecnológico empresarial. Esto obliga a la reflexión y la tendencia va en crecimiento. Sin embargo, la cultura de seguridad a nivel global en el país, no ha crecido en la ponderación esperada y eso no es bueno.

Para la organización frente a la ley 1273, leyes internacionales (SOX), debido proceso y omisión se han iniciado procesos estratégicos de seguridad tales como:

Estrategia de seguridad anual, aprobada y divulgada por la directiva de la compañía.

Talleres y programas permanentes de cultura de seguridad de la información a todos los miembros de la organización.

Mantenimiento del sistema de gestión de la protección de la información, controles y procedimientos.

Divulgación del código de conducta y las políticas de seguridad aceptadas, publicadas y firmadas por los miembros y trabajadores de la empresa (incluye terceros).

Clausula contractual (relación empresa-terceros) en el desarrollo de actividades y proyectos tecnológicos, en el incumplimiento de las políticas de seguridad.

De las utilidades de la compañía se asigna un porcentaje en las inversiones y servicios de seguridad de la información, con el objeto de mitigar los riesgos.

Implementación del centro de operación de Seguridad (SOC).

Implementación de laboratorio forense informático.

No obstante, el esfuerzo permanente está en la educación de todos los miembros de la organización en el cumplimiento de las políticas de seguridad, sus sanciones e impacto.

Se resalta que el éxito frente a este mal está en elaborar e implementar el sistema de gestión de seguridad de la información, en donde los directivos de la compañía deben dar apoyo. En caso contrario, no vale la pena hacer inversiones, toda vez que los resultados no son los esperados.

RS: Ciberseguridad y ciberdefensa son dos conceptos emergentes en la actualidad. ¿Cuál debería ser la posición del CISO frente a esta realidad? ¿Qué recomendaciones debe ofrecer a la organización en estos temas?

CAZS: Aunque es una realidad, está por encima del ámbito corporativo imposible de desconocer y, de manera directa, los CISO deben prepararse y conocer la tendencia mundial.

Desde mi punto de vista considero que con la cultura de seguridad lo que podemos hacer es crear concientización, para evitar que la compañía sea usada para atacar de manera masiva a un organismo, a una entidad o a la red de un país, dentro del marco de terrorismo en cualquiera de sus manifestaciones.

Un aporte es estar preparados y capacitarnos en cualquier evento que pueda afectar la operación de la compañía. Es importante tener en cuenta que no nace de una película de ciencia ficción, sino de una realidad en la que se descubre que los países, sus sistemas, sus redes económicas, sus valores comerciales, sus defensas y su movilidad están relacionados directamente con la tecnología que, al ser atacada, los afecta económicamente.

Fuga de información

Rafael H. Gamboa B.

Control de herramientas informáticas y responsabilidad legal

De un tiempo para acá el entorno empresarial ha cambiado muchísimo. Hasta hace unos pocos años, la comunicación se hacía mediante cartas en papel, documentos [1], y la información era almacenada, de manera física, en grandes espacios, con los consecuentes riesgos de estos procedimientos.

Tratos previos, ofertas, aceptaciones, contratos, otrosíes, pólizas y la contabilidad, entre otros, engrosaban los archivadores, los cuales en su gestión presentaban fallas en el acceso y en su seguridad.

Con el advenimiento de la tecnología, movilidad e interconectividad, así como de la desmaterialización de la información, los procesos se volvieron mucho más rápidos y eficientes, pero a la vez, el volumen de la información creció exponencialmente por la velocidad en las comunicaciones, generando que su control, sea cada vez más difícil.

Las organizaciones enfrentan el dilema sobre cómo controlar la información que les es valiosa, sin que en el camino se vulneren los derechos constitucionales que tienen sus empleados. Adicionalmente, cómo pueden prevenir conductas que redunden en una responsabilidad de la empresa.

Aspectos como las solicitudes particulares, órdenes judiciales, la privacidad e intimidad de los empleados en el uso de las herramientas electrónicas, llevan a las organizaciones a adoptar medidas que, respetando el ordenamiento, garanticen que no se van a ver perjudicadas las empresas, por acción u omisión de su recurso humano.

Información y herramientas

En el presente escrito cuando nos referimos a "información", nos estamos refiriendo a todo aquello que refleja, bien sea visual o audiblemente, el desarrollo de la empresa.

Secretos industriales, negociaciones con proveedores y empleados, "políticas" internas de la empresa, cámaras de seguridad, rastreo y seguimiento de actividad laboral entre otras, son algunas de las informaciones, que pueden afectar a la

organización, desde el punto de vista comercial, así como de su propia imagen.

Es usual que las empresas entreguen a sus empleados, tarjetas de acceso, portátiles, dispositivos inteligentes, USBs, acceso a internet, cuenta de correo electrónico, para el mejor desempeño de sus funciones, el problema surge cuando estas herramientas entregadas se usan para fines personales, ajenos a su actividad laboral.

En este punto, la pregunta es ¿cómo se hace para saber que las herramientas están siendo correctamente utilizadas? ¿Quién controla esto? La respuesta, es el Departamento de IT, toda vez que serán ellos los encargados de atender los requerimientos de la gerencia, para supervisar el correcto uso.

Lo anterior nos lleva a concluir que en la actualidad un área bien importante de una organización, es la de IT. Así mismo, que el área más "peligrosa" de una organización es la de IT. Y, por consiguiente, surge el interrogante sobre ¿quién controla al área de IT? … ¡Nadie!

La citada "peligrosidad" del área de IT, más que generar temores, representa una oportunidad para las organizaciones, de tener no sólo excelentes profesionales, sino además personas leales, pulcras y transparentes en su actuar.

A través de sistemas informáticos, cada vez es más fácil saber si un empleado está haciendo su trabajo y qué tan productivo es. Las tarjetas de acceso o los celulares o dispositivos equipados con GPSs, nos muestran el desplazamiento del empleado junto con la hora, día y permanencia en cada lugar.

El acceso a la red de la empresa o a Internet provisto por la organización, empleando el equipo de la oficina, el portátil suministrado o aún un dispositivo propio, puede indicar de una manera clara y exacta los sitios y duración de las visitas que realiza el empleado, sean relacionados o no con su trabajo, tales como correos electrónicos personales, redes sociales, casinos en línea entre otros.

Está establecido, mediante acuerdo entre la empresa y el empleado, que la cuenta de correo electrónico de la organización, además de la red y el acceso a internet anteriormente mencionado, deben ser exclusivamente usados con fines laborales, pero ¿cómo hace la empresa para saber que se está cumpliendo lo establecido, sin vulnerar los derechos que tiene el empleado? O peor aún, ¿cómo sabe una empresa que su empleado no está utilizando herramientas electrónicas para cometer ilícitos o sacar información valiosa de la empresa?

Alojamiento de pornografía infantil, de material protegido por los derechos de autor, uso de infraestructura computacional para realizar ataques o actividades ilícitas o simple fuga de información valiosa, pueden repercutir en gravísimas consecuencias para la organización, más aún, si ésta no adoptó las medidas necesarias para evitar que sucedieran las conductas anteriormente mencionadas.

Dentro de una investigación o de una instancia judicial, el investigador o el juez, analizará la diligencia con que actuó la empresa para evitar el tema investigado. Si se prueba que no adoptó medida alguna, será considerada su actitud como negligente, pudiéndosele encontrar responsable.

¿Puede o debe la organización adoptar medidas para evitar ser responsable por actividades de sus empleados en el uso de las herramientas electrónicas? La respuesta es un contundente SÍ.

Pronunciamientos jurisprudenciales en Colombia

En Colombia hay pronunciamientos judiciales donde el juez ha analizado la actitud que ha tenido el empleador frente a sus empleados, así como de terceros frente a la información de la empresa, en el uso de las herramientas electrónicas.

A continuación se mencionan los casos más significativos en los escenarios en donde se incluye la norma aplicable, el caso en concreto, la decisión adoptada y los comentarios del caso.

Solicitud vía derecho de petición de información por parte de particulares.

La Norma:

"*ARTICULO 23. De la Constitución Nacional. Toda persona tiene derecho a presentar peticiones respetuosas a las autoridades por motivos de interés general o particular y a obtener pronta resolución. El legislador podrá reglamentar su ejercicio ante organizaciones privadas para garantizar los derechos fundamentales.*"

El Caso:

Un particular, sin vinculación alguna de la empresa, vía derecho de petición consagrado en el artículo 23 de la Constitución Nacional, solicita información que reposa en el los archivos de la empresa.

Comentario:

Aunque originalmente la norma consagrada en el artículo 23 de la Constitución Nacional era para destinación de los funcionarios del Estado, vía jurisprudencia constitucional, se estableció que los particulares, están sometidos a la norma citada, siempre y cuando la no entrega de la información pueda acarrear una vulneración a cualquier derecho constitucional.

Debe analizarse la solicitud y sobre todo el potencial riesgo que haya con la entrega de la solicitada información.

Acceso no autorizado a una cuenta de correo.

La Norma:

"*ARTÍCULO 195 del Código Penal. El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa.*[2]"[3]

El Caso:

Exempleado, con base en el artículo 195 del Código Penal, vigente para ese momento, denuncia penalmente al Administrador del correo de la empresa y al Vicepresidente de tecnología, ya que "abusivamente" ingresaron a su cuenta de correo de la empresa, la cual estaba protegida con una "medida de seguridad" (contraseña).

La decisión:

El 28 de octubre de 2004, la Fiscalía 57 local delegada ante los Jueces Penales Municipales, precluyó la investigación

por no haber acto "abusivo", no haberse violado medida de seguridad.

Comentario:

Efectivamente, entre el empleado y la empresa había un acuerdo y términos de uso en donde se establecía expresamente que el correo electrónico era para fines de la empresa y que el empleado no podía esperar privacidad.

Por otro lado, la fiscalía no encontró que se hubiere vulnerado medida de seguridad, ya que el administrador al ser "superusuario", no tenía necesidad de conocer o usar la contraseña de quien denunciaba.

Acceso no autorizado a imágenes alojadas en portátil de la empresa.

La Norma:

Intimidad y Buen Nombre. "*Artículo 15 de la Constitución Nacional. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo tiene derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.*"

Honra. "*Artículo 21 de la Constitución Nacional. Se garantiza el derecho a la honra. La ley señalará la forma de su protección.*"

El Caso:

Empleada, había almacenado imágenes de contenido sexual en el portátil que le había sido entregado por parte del empleador. La empleada le prestó el portátil a un compañero de trabajo, el cual informó al empleador de las imágenes. El empleador enterado de la situación, le solicita a la empleada su renuncia y ésta interpone una acción de tutela en contra de la empresa.

La decisión:

El 24 de mayo de 2007, la Corte Constitucional, protegió la intimidad, honra, buen nombre así como la autodeterminación sobre la imagen de la empleada y ordenó a la empresa la destrucción de las imágenes.

Comentario:

La Corte fundo su decisión en que, no obstante existir un acuerdo de destinar el equipo exclusivamente a aspectos laborales, las imágenes encontradas estaban en una carpeta denominada "mis imágenes", lo que implicaba el deseo de tener privacidad.

Requerimiento judicial de copia de correos electrónicos del servidor de una empresa.

La Norma:

Intimidad e Inviolabilidad de correspondencia. "*Artículo 15 de la Constitución Nacional. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo tiene derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.*

…La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley…"

El Caso:

Dentro de un trámite arbitral se solicitó como prueba la copia de los correos electrónicos tomados del servidor de la empresa. El Tribunal de Arbitramento decretó la prueba, ante lo cual, los empleados de la empresa de donde se tomarían los correos electrónicos, interpusieron tutela en contra del Tribunal de Arbitramento.

La decisión:

El 4 de septiembre de 2007, la Sala Civil de la Corte Suprema de Justicia, no tuteló los derechos reclamados, toda vez que no se vulnera la intimidad o la inviolabilidad de la correspondencia cuando existe un mandato legal.

Comentario:

Este caso es un claro ejemplo que cuando existe una orden judicial, ésta debe ser acatada. En la misma decisión, se ordenó además, hacer un filtro, para que los correos electrónicos tuvieran relación con los temas del proceso judicial.

Correos electrónicos aportados a un proceso sin autorización judicial.

La Norma:

Intimidad. "*Artículo 15 de la Constitución Nacional. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo tiene derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas…*"

Debido Proceso. "*Artículo 29 de la Constitución Nacional. El debido proceso se aplicará a toda clase de actuaciones judiciales y administrativas…*".

Acceso afectivo a la Administración de Justicia. *"Artículo 229 de la Constitución Nacional. Se garantiza el derecho de toda persona para acceder a la administración de justicia. La ley indicará en qué casos podrá hacerlo sin la representación de abogado.*"

El Caso:

Dentro de un proceso de divorcio, la mujer aportó en un interrogatorio de parte, correos electrónicos tomados del computador y de la cuenta que compartía la pareja. Ante tal situación, el perjudicado interpuso acción de tutela en contra del Juez para que desestimaran los correos aportados.

La decisión:

El 18 de septiembre de 2008, la Corte Constitucional protegió la intimidad, el debido proceso y el efectivo acceso a la administración de justicia, por correos obtenidos sin autorización judicial.

Comentario:

Al haberse aportado correos electrónicos sin que hubiere medido una orden judicial, ningún juez puede tenerlos en cuenta. Lo anterior no obsta para que de manera oficiosa, el juez decrete pruebas encaminadas a descubrir la verdad y generar convencimiento, para proferir una sentencia.

Desarrollos internacionales

A nivel internacional ya es pacífica la jurisprudencia y la ley que, como consecuencia de las múltiples condenas a las empresas, previo acuerdo con los empleados y con "conocimiento consenti-

do", impongan los mecanismos que estimen pertinentes para proteger la propia información de la empresa, así como de eventuales responsabilidades en el ámbito, penal, civil y comercial.

En resumen, en países como los Estados Unidos, respecto de las herramientas electrónicas entregadas al empleado por la empresa, existe un principio que los empleados no pueden esperar la más mínima privacidad o confidencialidad y en caso de sospecha de alguna actividad, que perjudique o pueda perjudicar a la empresa, se aplica la política de "cero tolerancia".

Conclusiones

Actualmente en Colombia, ante la ausencia de orden judicial, la Jurisprudencia constitucional es unánime en proteger la intimidad y confidencialidad de los empleados, así medie acuerdo entre las partes de no existir tales derechos.

La anterior situación va a tener necesariamente que cambiar, toda vez que como ocurrió en otras latitudes, la empresa debe protegerse y hacer cumplir la ley, lo cual sólo se puede garantizar de una manera eficiente y diligente, mediante la aplicación y empleo de herramientas tecnológicas de control.

Finalmente, la gran disyuntiva del empresario colombiano es, no supervisar para evitar condenas vía tutela, o supervisar y someterse a una condena adversa. En el primer escenario el empresario expone sus más importantes activos por la posibilidad de fuga y una eventual responsabilidad de la empresa; y en el segundo escenario, correrá la posibilidad de fuga, de responsabilidades y si es demandado vía tutela, la orden del juez será cesar en la actividad vulneradora de los derechos constitucionales.

¿Cuál escoge usted?

Notas al pie de Página

[1] El Código General del Proceso, en estudio en el Congreso, define en su artículo 243, las distintas clases de documentos así: "Artículo 243.- Distintas clases de documentos. Son documentos los escritos, impresos, planos, dibujos, cuadros, mensajes de datos, fotografías, cintas cinematográficas, discos, grabaciones magnetofónicas, videograbaciones, radiografías, talones, contraseñas, cupones, etiquetas, sellos y, en general, todo objeto mueble que tenga carácter representativo o declarativo, y las inscripciones en lápidas, monumentos, edificios o similares."

[2] Este artículo fue modificado el artículo 25 de la ley 1288 de 2009 (declarada inexequible el 16 de noviembre de 2010), el cual fue derogado por el artículo 4 de la ley 1273 de 2009.

[3] Una norma similar es la que se encuentra vigente en el artículo 269 A del Código Penal

Rafael Hernando Gamboa Bernate. *Abogado, Pontificia Universidad Javeriana de Bogotá. Master en leyes (LL.M.) en Tecnologías de la Información y Privacidad de The John Marshall Law School Chicago. Master en leyes (LL.M.) en Propiedad Intelectual de The John Marshall Law School Chicago. Ha sido Profesor de posgrado en las universidades de los Andes, UPB Bucaramanga, UPB Medellín, Antioquia, Javeriana Bogotá, Externado, El Rosario, La Sabana, Sergio Arboleda. Trabajó con el Centro de Arbitraje y Conciliación de la Cámara de Comercio de Bogotá; con Caracol y RCN Televisión. Actualmente es miembro de la oficina de Abogados Bernate & Gamboa Abogados.*

Seguridad Infórmatica en Colombia Tendencias 2010-2011[1]

Andrés Ricardo Almanza Junco

Comienza una nueva década con otras realidades y retos en temas de seguridad de la información en nuestro país. Una etapa en la que el camino en temas de protección de la información, está dentro de la agenda corporativa de las organizaciones. Se espera que esta nueva década de desafíos alrededor de la seguridad de la información, siga siendo algo importante en nuestro país, y Latinoamérica, que exija a todos los responsables de estos asuntos en las empresas, un esfuerzo máximo, orientado a la protección de la información.

Este año la participación en la XI Encuesta Nacional de Seguridad Informática fue de 215 personas de los diferentes sectores productivos del país, en el tema de seguridad de la información. En esta ocasión como en el año anterior se han vinculado Uruguay, Argentina, Paraguay, Venezuela y México, países que han querido adelantar este mismo ejercicio. Los resultados estarán disponibles en el sitio web de la Asociación Colombiana de Ingenieros de Sistemas, ACIS.

El análisis presentado a continuación se desarrolló basado en una muestra aleatoria que respondió una encuesta de manera interactiva, a través de la página web dispuesta por ACIS para tal fin. Dadas las limitaciones de tiempo y recursos disponibles en la Asociación, se ha realizado un conjunto de análisis básicos, los cuales pretenden ofrecer los elementos más sobresalientes de los resultados obtenidos, con el propósito de orientar al lector sobre las tendencias identificadas en el estudio.

Con esto en mente y considerando otros estudios internacionales como el *2011 Global State of Information Security Study* de Pricewaterhousecoopers –PwC-; The Future of Security de Deloitte; y, 2011 Strategic Security de informationweek, se procederá a analizar los resultados de la Encuesta Nacional de Seguridad Informática ACIS 2010-2011.

Estructura de la encuesta

Fue diseñado un cuestionario compuesto por 35 preguntas sobre los siguientes temas:

- Demografía
- Presupuestos
- Fallas de seguridad

- Herramientas y prácticas de seguridad
- Políticas de seguridad
- Capital Intelectual

Demografía

Esta sección identifica los siguientes elementos

- Zona geográfica
- Sector de la organización
- Tamaño de la organización
- Responsabilidad y responsables de la seguridad
- Ubicación de la responsabilidad en la organización

Presupuestos

Esta parte muestra si las organizaciones han destinado un rubro para la seguridad informática, y su valor anual. Permite revisar el tipo de tecnología en el que invierten y un estimado del monto de la inversión en seguridad informática.

Fallas de seguridad

Esta sección revisa los tipos de fallas de seguridad más frecuentes; cómo se enteran sobre ellas y a quién las notifican. Por otra parte, identifica las causas por las cuales no se denuncian y si existe la conciencia sobre la evidencia digital en la atención de incidentes de seguridad informática.

Herramientas y prácticas de seguridad informática

En este segmento de la encuesta, el objetivo es identificar las prácticas de las empresas sobre la seguridad, los dispositivos o herramientas que con más frecuencia utilizan para el desarrollo de la infraestructura tecnológica, y las estrategias que utilizan las organizaciones para enterarse de las fallas de seguridad.

Políticas de seguridad

Esta sección busca indagar sobre la formalidad de las políticas de seguridad en la organización; los principales obstáculos para lograr una adecuada seguridad; la buenas prácticas o estándares que utilizan; los contactos nacionales e internacionales para seguir posibles intrusos.

Capital Intelectual

Finalmente, esta sección analiza la situación de desarrollo profesional en torno a conocimientos relacionados con tareas propias de tecnologías de la información: personal dedicado a esta tarea, personal certificado, importancia de las certificaciones y años de experiencia en el rubro de seguridad informática.

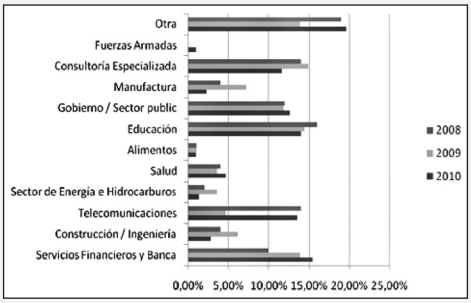
Consideraciones muestrales

Considerando una población limitada (alrededor de 2093 personas que participan activamente en la lista de seguridad SEGURINFO), se ha estimado un error muestral de 7% (confianza del 93%), lo cual nos permite manejar una muestra adecuada, cercana a los 183 participantes. Al contar con 215 participantes en la muestra, los resultados presentados son estadísticamente representativos.

A continuación se presentan los resultados (en porcentajes) de la encuesta por temas y algunos comentarios relacionados con los datos obtenidos.

Demografía

Sectores participantes:

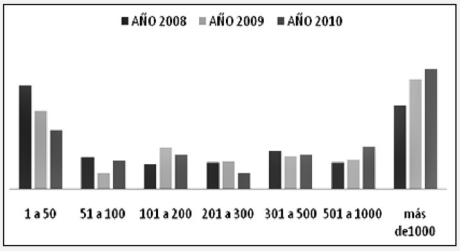


	2010	2009	2008
Servicios Financieros y Banca	15,42%	13,92%	10,00%
Construcción / Ingeniería	2,80%	6,19%	4,00%
Telecomunicaciones	13,55%	4,64%	14,00%
Sector de Energía e Hidrocarburos	1,40%	3,61%	2,00%
Salud	4,67%	3,61%	4,00%
Alimentos	0,93%	1,03%	1,00%
Educación	14,02%	14,43%	16,00%
Gobierno / Sector public	12,62%	11,86%	12,00%
Manufactura	2,34%	7,22%	4,00%
Consultoría Especializada	11,68%	14,95%	14,00%
Fuerzas Armadas	0,93%	0,0%	0,0%
Otra	19,63%	13,92%	19,00%

Comentarios generales:

Los resultados muestran una participación activa de la banca, el sector educativo, el gobierno, las telecomunicaciones y el sector de la consultoría especializada; cuatro sectores donde de acuerdo con las tendencias internacionales se viene manifestando la necesidad de contar con una directriz formal en temas de seguridad de la información. Adicionalmente, es importante anotar las regulaciones que rigen en nuestro país en el sector financiero, generadoras generadores de cambios en dicho sector.

Número de empleados de la Organización

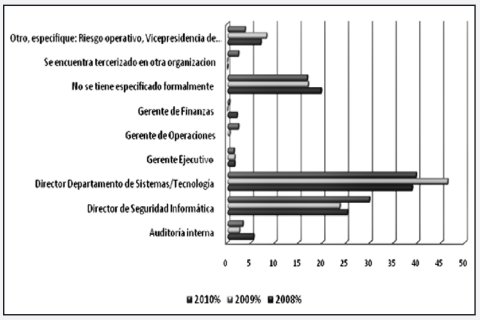


	AÑO 2008%	AÑO 2009%	AÑO 2010%
1 a 50	31,03	23,50	17,76
51 a 100	9,36	4,64	8,41
101 a 200	7,39	12,37	10,28
201 a 300	7,88	8,25	4,67
301 a 500	11,33	9,79	10,28
501 a 1000	7,88	8,76	12,62
más de1000	25,12	32,99	35,98

Comentarios generales:

Al igual que en años anteriores, la mediana y grande industria participan con porcentajes importantes en la encuesta. Tendencias nacionales e internacionales, muestra la importancia de la seguridad de la información, que sigue convirtiéndose en un elemento clave para la formalización de sus estrategias de negocio. Hoy es parte de las estrategias corporativas, está centrada en mezclar una agilidad de su negocio, con la confianza de la información que se posee para lograr el resultado.

Dependencia organizacional del área de seguridad informática

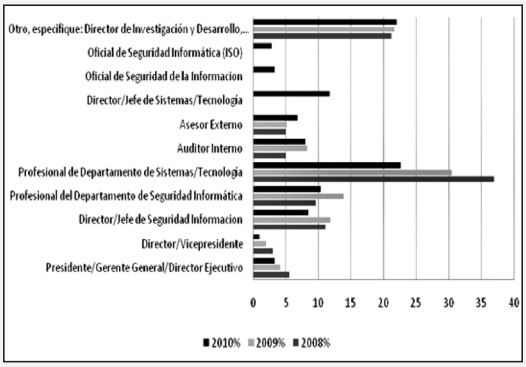


	2008 %	2009%	2010%
Auditoria interna	5,56	2,58	3,27
Director de Seguridad Informática	25,25	23,71	29,91
Director Departamento de Sistemas/Tecnología	38,89	46,39	39,72
Gerente Ejecutivo	1,52	1,55	1,40
Gerente de Operaciones		0,52	2,34
Gerente de Finanzas	2,02	0	0,47
No se tiene especificado formalmente	19,7	17,01	16,82
Se encuentra tercerizado en otra organización	-	-	2,34
Otro, especifique: Riesgo operativo, Vicepresidencia de Operaciones, Jefe de Telemática, etc.	7,07	8,25	3,74

Comentarios generales:

Los resultados de este año muestran un aumento significativo del cargo Director del área de Seguridad Informática. Indica que disminuye moderadamente las organizaciones que no tienen formalmente especificada la dependencia del tema de seguridad de la información. Según se observa en los datos, la seguridad de la información continúa ganando terreno, pero es necesario afinar el discurso, tanto de las áreas de seguridad como de tecnología, para que sus propuestas se afinen con los procesos de negocio y no estrictamente con los elementos tecnológicos y de infraestructura, dado que esta área continúa teniendo un matiz eminentemente tecnológico y operacional, lo que limita su participación en decisiones de negocio o estrategias de las organización. Las tendencias internacionales y locales también muestran la necesidad de crear un gobierno al respecto de la seguridad y por esto es un cargo en aumento, que se ha ido creando en los ambientes organizacionales.

Cargos que respondieron la encuesta



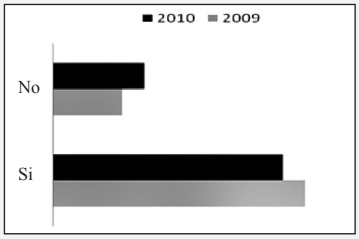
	2008 %	2009%	2010%
Presidente/Gerente General/Director Ejecutivo	5,56	4,12	3,29
Director/Vicepresidente	3,03	2,06	0,94
Director/Jefe de Seguridad Información	11,11	11,86	8,45
Profesional del Departamento de Seguridad Informática	9,60	13,92	10,33
Profesional de Departamento de Sistemas/Tecnología	36,87	30,41	22,54
Auditor Interno	5,05	8,25	7,98
Asesor Externo	5,05	5,15	6,75
Director/Jefe de Sistemas/Tecnología	-	-	11,74
Oficial de Seguridad de la Información	-	-	3,29
Oficial de Seguridad Informática (ISO)	-	-	2,82
Otro, especifique: Director de Investigación y Desarrollo, Investigador criminalístico, Gerente de proyectos, Consultor de seguridad.	21,21	21,65	22,07

Comentarios generales:

Este año se tiene una disminución de los profesionales de TI, que responden por la seguridad, pero notamos que cargos como el ISO o el CISO responden de manera importante. Esto nos indica la responsabilidad de las organizaciones con el tema de la seguridad de la información, y la necesidad de tener un responsable directo del tema, máxime cuando uno de los ítems importantes de los temas de gobernabilidad de las organizaciones, son los roles y las responsabilidades bien definidas. De igual forma, la participación de la alta gerencia, a pesar de ser limitada en los resultados de este año, continúa presente y denotando que el tema es de su interés, pero en el contexto del negocio. De nuevo se insiste en la necesidad de abrir espacios de comunicación bidireccionales, entre la gerencia del negocio y la seguridad de la información, para avanzar en una reflexión coordinada que beneficie tanto a la organización como al área de seguridad, pensando en la gobernabilidad de dos mundos que hoy por hoy poseen unas relaciones demasiado estrechas.

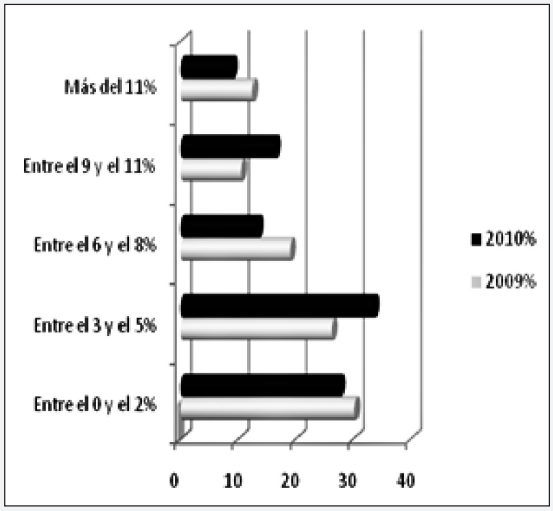
Presupuesto

¿El presupuesto global de su organización, incluye aspectos de seguridad de la información, y cuál es el valor porcentual del presupuesto global?



	2009	2010
Si	78,35%	71,50
No	21,65%	28,50

Valores porcentuales de la inversión cuando se hace.



	2009 %	2010 %
Entre el 0 y el 2%	30,26	27,61
Entre el 3 y el 5%	26,32	33,58
Entre el 6 y el 8%	19,08	13,43
Entre el 9 y el 11%	10,53	16,42
Más del 11%	12,50	8,96

Comentarios generales:

Desde el año anterior esta pregunta se ha introducido con el propósito de observar qué tanto se invierte del presupuesto en los temas de seguridad de la información. Es importante resaltar que si se invierte en el tema de seguridad de la información en las organizaciones, es una tendencia que muestra el entendimiento de protegerla. Al observar las cantidades invertidas vemos que más del 70% de las respuestas muestran inversiones, y al llevarlo al desglose de la cantidad del presupuesto vemos para este año un aumento importante en los valores, del 3 al 5% del mismo, mostrando una tendencia conservadora en los temas de protección. Por otro lado, un crecimiento en la inversión entre el 9 y 11 % del presupuesto, lo que indica una creciente preocupación por la protección de la información. De igual manera esto se ve en las empresas grandes que están realizando más inversión, dada la fragilidad de la información de sus negocios.

¿En qué temas se concentra la inversión en seguridad informática?

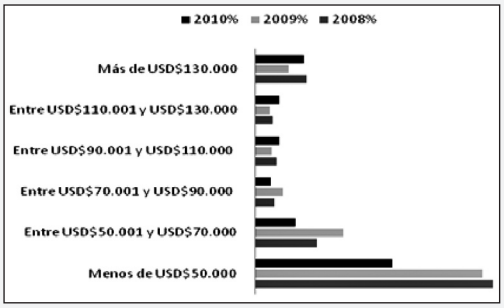
	2008 %	2009 %	2010%
Protección de la red	75,9	81,4	53,27
Proteger los datos críticos de la organización	61,1	69,1	42,99
Proteger la propiedad intelectual	30	24,2	13,55
Concientización/formación del usuario final	33,5	26,8	19,63
Comercio/negocios electrónicos	21,2	14,4	7,94
Desarrollo y afinamiento de seguridad de las aplicaciones	31	24,2	37,38
Contratación de personal más calificado	11,3	12,4	14,49
Evaluaciones de seguridad internas y externas	25,1	25,3	19,16
Monitoreo de Seguridad Informática 7x24	25,6	23,7	15,42
Cursos especializados	25,6	18,6	17,29
Pólizas de cibercrimen	4,43	5,2	1,87
Desarrollo de políticas y procedimientos de seguridad	-	-	28,97
Cumplimiento de exigencias legales y/ corporativas en cuanto a seguridad de (entes reguladores, SOX, ISO 27000, etc.)	-	-	20,09
Otro, especifique: Ninguno, Capacitación, auditoría, certificaciones de seguridad, continuidad del negocio	6,4	3,1	1,40

Comentarios generales:

Los resultados de este año muestran una disminución en la tendencia de la inversión en seguridad concentrada en la zona perimetral, en las redes y sus componentes, así como en la protección de datos críticos de la organización. Llama

la atención un mejoramiento de inversiones en desarrollo y de la seguridad de las aplicaciones, así como la aparición de dos aspectos, por un lado inversión en el cumplimiento de regulaciones, así como desarrollo de políticas de seguridad de la información, como elementos emergentes que se empiezan a imponer a nivel nacional. Los demás ítems en sus debidas proporciones tienen disminuciones que se reafirman con las encuestas internacionales, donde pese a la crisis económica mundial se mantienen con disminuciones moderadas, las inversiones en las diferentes temáticas de protección de información.

Presupuesto previsto para Seguridad Informática 2010



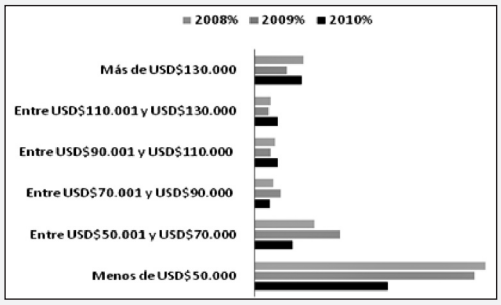
	2008 %	2009 %	2010 %
Menos de USD$50.000	58,33	55,7	33,58
Entre USD$50.001 y USD$70.000	15,10	21,6	9,70
Entre USD$70.001 y USD$90.000	4,69	6,7	3,73
Entre USD$90.001 y USD$110.000	5,21	4,1	5,97
Entre USD$110.001 y USD$130.000	4,17	3,6	5,97
Más de USD$130.000	12,50	8,2	11,94

Comentarios generales:

Es interesante ver este año una leve disminución de la inversión en seguridad en la franja menor de los USD$70.000, pero se siguen presentando crecimientos importantes, por encima de los USD$90.000. Esto se apalanca en la cantidad de normativas y regulaciones alrededor de la industria nacional que generan una mayor inversión de recursos en temas de protección de la información. En las demás franjas de inversión se ve una disminución leve, a excepción de la franja de los USD$130.000, que puede ser producto de los efectos de las crisis económicas mundiales y de que en años anteriores fueron realizadas inversiones de este tipo que hoy se pueden mantener con unos niveles más bajos.

La encuesta de seguridad realizada por *PriceWaterHouseCoopers Global Information Security State 2011,* muestra que las empresas norteamericanas disminuyeron su inversión en seguridad informática. Se nota una preocupación por los temas de Continuidad de Negocio, Reputación, y Cumplimiento como los drivers más importantes en los gastos de seguridad de la información, eso reafirma los resultados de Colombia, en cuanto a la tendencia de disminuir el gasto en la protección de la red e inversión, menores de USD$50.000, dado que los otros drivers requieren de mayores inversiones, como los temas de Desarrollo de Políticas de Seguridad, y Cumplimiento con normativas y regulaciones.

Presupuesto previsto para Seguridad Informática 2011



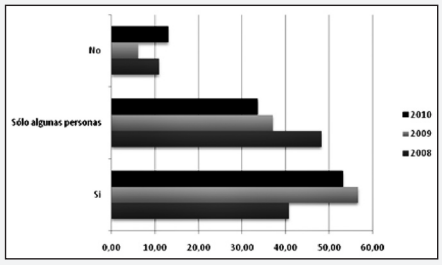
	2008 %	2009%	2010%
Menos de USD$50.000	50,52	49,48	31,34
Entre USD$50.001 y USD$70.000	19,27	19,07	10,45
Entre USD$70.001 y USD$90.000	7,29	11,34	6,72
Entre USD$90.001 y USD$110.000	5,73	4,64	3,73
Entre USD$110.001 y USD$130.000	5,73	3,61	7,46
Más de USD$130.000	11,46	11,86	14,93

Comentarios generales:

Las proyecciones de las organizaciones en los temas de inversión en seguridad sugieren unos incrementos leves para el 2011; se nota un incremento considerable en la franja de los $USD90.000 en adelante, el cual se orienta fundamentalmente a cumplir con normatividad de obligatorio seguimiento, certificaciones de procesos de misión crítica y temas de pólizas de seguro, frente a asuntos de cibercriminalidad, desarrollo de políticas de seguridad de la organización. Estas inversiones generalmente desarrolladas por la Banca, el sector de telecomunicaciones y las grandes empresas, establecen un referente base para la dinámica empresarial del país, que le indica a cada uno de los sectores productivos que la seguridad de la información, no es un tema de los "informáticos" y requiere el concurso de la gerencia y el área de tecnología de la información, para alcanzar las metas propuestas.

En el informe 2011 Global State of Information Security Study de Pricewaterhousecoopers, sobresalen como direccionadores de la inversión en seguridad, la continuidad de negocio, el cumplimiento de regulaciones y normativas internas y externas, y la protección de la reputación de la empresa, las limitaciones sobre los presupuestos destinados a protección de la información, que han obligado a los gerentes de seguridad a ser selectivos con los programas definidos en procura de la protección de la información.

Reconocimiento por parte de la organización de la información como un activo a proteger



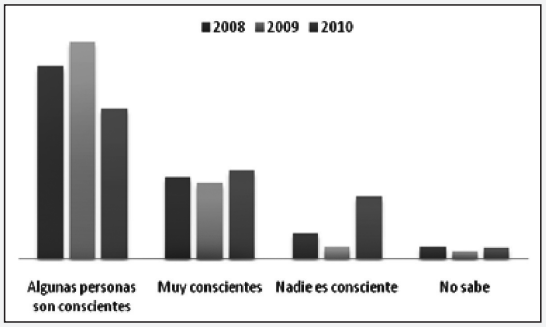
	2008	2009 %	2010%
Si	40,80%	56,70%	53,27
Sólo algunas personas	48,20%	37,11%	33,64
No	11,00%	6,19%	13,08

Comentarios generales:

Este cuestionamiento muestra que, a pesar de existir una baja en los números, es evidente que quienes contestaron la encuesta entienden que la información como un activo posee valor dentro de la organización y, por lo tanto, se convierte en un activo que debe ser protegido. De igual manera se reitera la necesidad de seguir realizando esfuerzos importantes en la forma en cómo se toma conciencia de la información como hilo conductor en los negocios, debe ser este uno de los elementos claves a la hora de prestar servicios y, por tanto, su protección se hace cada vez más notoria; en consecuencia, la articulación de las unidades de negocio y la seguridad deben ser un reto a la hora de entender la labor relacionada con la información de la organización.

Fallas de seguridad

Conciencia en Seguridad de la Información y el uso de buenas prácticas

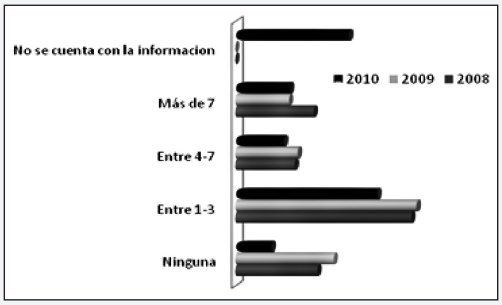


	2008	2009	2010
Algunas personas son conscientes	61,60	69,49	48,21
Muy conscientes	26,10	24,29	28,21
Nadie es consciente	8,40	3,95	20,00
No sabe	3,90	2,26	3,59

Comentarios generales:

La tendencia nos muestra cómo las organizaciones poco a poco han venido abordando la seguridad de la información y el uso de buenas prácticas en la protección de la misma, un aumento importante en la falta de conciencia y poco interés frente al uso de las buenas prácticas, que puede deberse al estatu quo que algunas organizaciones han alcanzado luego de la presencia de las normativas y regulaciones, que nuestro ambiente nacional ha venido generando, durante los últimos periodos. De todas formas hay que resaltar que la conciencia colectiva frente a los temas de buenas prácticas en seguridad de la información existen, más aún, con los escenarios y casos tan sonados a los que el mundo se ha visto expuesto.

Intrusiones o incidentes de seguridad identificados en el año

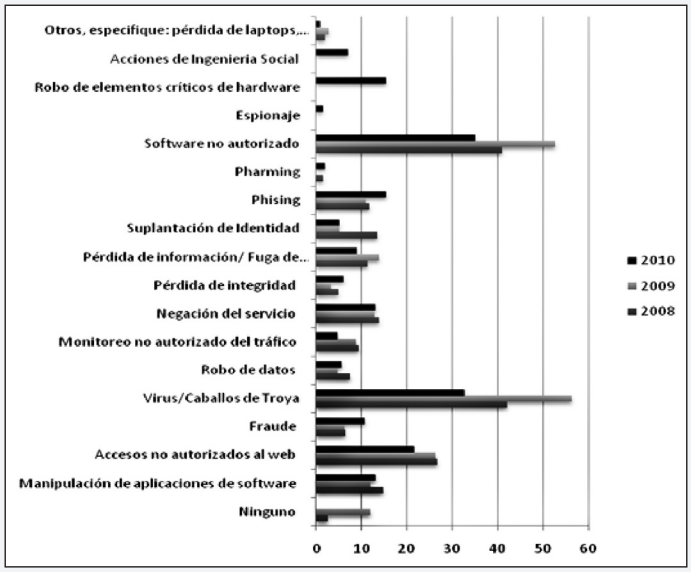


	2008	2009	2010
Ninguna	20,70	24,86	9,23
Entre 1-3	44,40	45,76	35,90
Entre 4-7	15,00	15,82	12,31
Más de 7	19,80	13,56	13,85
No se cuenta con la información	-	-	28,72

Comentarios generales:

Estos resultados muestran cómo las intrusiones se han venido identificando y tratando; más del 60% sí ha identificado algún tipo de intrusión, lo que indica que hay un monitoreo continuo que busca tratar de ser mayor reactivo frente a un panorama que no tiene un fin. Esto se refuerza en el *informe de PwC del 2011, el cual* manifiesta el decremento del desconocimiento de los incidentes que se presentan en las organizaciones y sobre todo aquellas de tipo financiero. Este panorama nos invita a fortalecer nuestros escenarios de protección de la información y a buscar el esfuerzo continuo para controlar las incidencias y disminuir su efecto dentro de las organizaciones. Se siguen prendiendo las alarmas frente a la necesidad de involucrar en las arquitecturas e infraestructuras de seguridad de la información, el monitoreo para identificar los posibles eventos que afecten a los negocios, desde el punto de vista de la seguridad.

Tipos de fallas de seguridad



Continúa

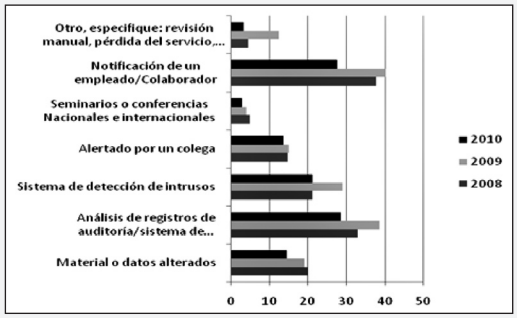
	2008	2009	2010
Ninguno	2,46	11,9	-
Manipulación de aplicaciones de software	14,8	11,9	13,08
Accesos no autorizados al web	26,6	26,3	21,50
Fraude	6,4	6,2	10,75
Virus/Caballos de Troya	41,9	56,2	32,71
Robo de datos	7,39	4,6	5,61
Monitoreo no autorizado del tráfico	9,36	8,8	4,67
Negación del servicio	13,8	12,9	13,08
Pérdida de integridad	4,93	3,1	6,07
Pérdida de información/ Fuga de Información	11,3	13,9	8,88
Suplantación de Identidad	13,50	5,2	5,14
Phising	11,8	10,8	15,42
Pharming	1,48	0,0	1,87
Software no autorizado	40,9	52,6	35,05
Espionaje	-	0,0	1,40
Robo de elementos críticos de hardware	-	-	15,42
Acciones de Ingeniería Social	-	-	7,01
Otros, especifique: pérdida de laptops, acceso no autorizado a equipos, fuga de información, spyware.	1,97	2,7	0,93

Comentarios generales:

Este año se observan unas variaciones importantes; mientras por un lado disminuye la presencia de Virus/Caballos de Troya, situación que muestra los esfuerzos de las organizaciones en mejorar sus controles técnicos de contención frente a estas amenazas, otros escenarios aumentan; el Phishing, Robo de datos, Perdida de Integridad, así como el Fraude, y la manipulación de aplicaciones de software, lo que muestra que la forma de afectar a las organizaciones está cambiando. Se observa cómo los ataques dirigidos son latentes y buscan generar mayores efectos sobre la información de las organizaciones; son una tendencia en la realidad nacional reforzada con los eventos que de manera internacional se han presentado durante el último año. De igual manera, han entrado unas nuevas categorías, como las acciones de Ingeniería Social, así como el robo de elementos de hardware, con algunos valores importantes, mostrando otra cara de la moneda, no basta proteger los datos, también es importante los temas de seguridad y protección física.

Es importante llamar a los diferentes sectores desarrolladores, administradores y el nivel de gestión para realizar un frente común de protección, donde se escriban códigos pensados en la seguridad de las aplicaciones, administración de plataformas que contemplen la administración de seguridad dentro de sus procedimientos, y la gestión con un modelo estructurado que pueda medir la efectividad de las medidas de protección que la organización está implementando.

Identificación de las fallas de seguridad informática



	2008	2009	2010
Material o datos alterados	20,1	19,1	14,49
Análisis de registros de auditoría/sistema de archivos/registros Firewall	33	38,7	28,50
Sistema de detección de intrusos	21,18	28,9	21,30
Alertado por un colega	14,77	14,9	13,55
Seminarios o conferencias Nacionales e internacionales	4,92	4,1	2,80
Notificación de un empleado/Colaborador	37,80	40,2	27,57
Otro, especifique: revisión manual, pérdida del servicio, auditorias	4,43	12,4	3,27

Comentarios generales:

Vemos cómo las tecnologías reactivas o de protección de perímetro se mantienen como las fuentes primarias para la detección de posibles fallas de seguridad en las infraestructuras de computación; un dato importante señala que se mantiene igual la notificación por parte de terceros, o colegas sobre las posibles fallas de seguridad, mostrando que los intercambios de información como Segurinfo siguen siendo una tendencia a considerar, para enterarse de las fallas de seguridad. Se prenden las alarmas al ver cómo disminuye el análisis de registros, o de auditoría. Este llamado de atención se orienta a tener presente que dentro del mundo complejo de la seguridad de la información, una de las actividades de gran importancia es el monitoreo, que ayuda dentro de este posible escenario para identificar las posibles fallas de seguridad que se presentan dentro de la organización.

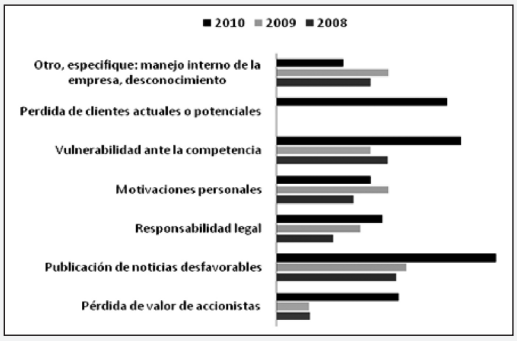
Notificación de un incidente de seguridad informática

	2008	2009	2010
Asesor legal	11,82	17,0	9,35
Directivos de la organización	-	-	56,07
Autoridades locales/ regionales	5,41	5,2	5,61
Autoridades nacionales	5,41	6,7	13,08
Equipo de atención de incidentes	24,63	40,2	18,69
Ninguno: No se denuncian	30,04	29,9	17,76
Otro	-	10,8	8,88

Comentarios generales:

Los datos de este año muestran un aumento importante en la vinculación de las autoridades nacionales en los temas asociados con incidentes de seguridad, esto es algo muy positivo, dado que refleja la confianza en los aparatos de administración de justicia. Muestra también una interrelación de la tecnología y los entes judiciales, y de manera indirecta una mayor comunicación con las áreas jurídicas las que, en últimas, se convertirán en las áreas que hagan seguimiento a este tipo de situaciones. Una alarma importante se observa en el decremento en los grupos de atención de incidentes, mientras que las tendencias internacionales, reflejan lo contrario, su crecimiento en la realidad nacional comparado con los años anteriores disminuye sustancialmente. Es importante resaltar que decrece el no denunciar, esto se ve reflejado en lo anteriormente mencionado de involucrar a las autoridades nacionales. Se muestra además, una nueva categoría que involucra a la alta gerencia o los niveles ejecutivos de la organización, los cuales reflejan interés por conocer estos temas, lo cual también indica una creciente tendencia por gestionar desde la dirección estos incidentes, que pueden afectar de manera importante a la organización. Es de resaltar la labor que actualmente adelanta la unidad de delitos informáticos de la DIJIN, en la Policía Nacional, así como sus semejantes en el DAS y en la Fiscalía General de la Nación.

Si decide no denunciar



	2008	2009	2010
Pérdida de valor de accionistas	6,93	6,7	24,77
Publicación de noticias desfavorables	24,27	26,3	44,39
Responsabilidad legal	11,56	17,0	21,50
Motivaciones personales	15,60	22,7	19,16
Vulnerabilidad ante la competencia	22,54	19,1	37,38
Pérdida de clientes actuales o potenciales	-	-	34,58
Otro, especifique: manejo interno de la empresa, desconocimiento	19,07	22,7	13,55

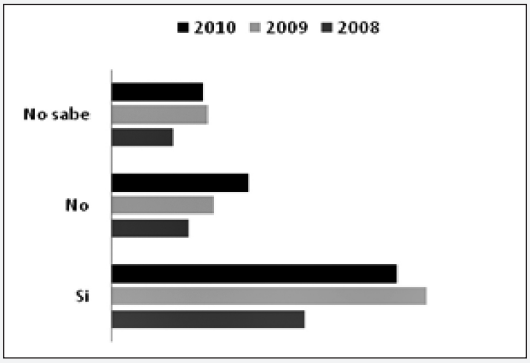
Comentarios generales:

La publicación de noticias desfavorables, la responsabilidad legal, vulnerabilidad ante la competencia, así como la pérdida de valor (reputación) ante accionistas, son las tendencias más significativas de los resultados de esta sección.

En este orden de ideas, la administración de riesgos de seguridad informática articulados con aquellos identificados para los procesos de negocio, debe ser un imperativo que produzca sistemas de gestión de seguridad y de proceso más resistente, resilente y confiable. Es importante anotar, que cada vez más se

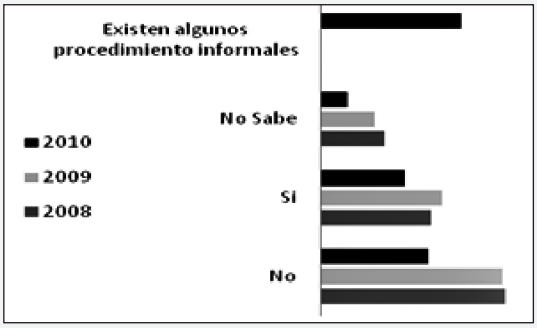
establecen legislaciones o estándares de aplicación obligatorios, como medidas para procurar un proceso continuado de administración de los riesgos de la seguridad de la información, algunos ejemplos la nueva norma de la Superfinanciera de Colombia sobre seguridad informática.

Conciencia de la evidencia digital, y su tratamiento en la atención de incidentes



	2008	2009	2010
Si	37,68	61,36	55,50
No	15,14	19,89	26,70
No sabe	11,97	18,75	17,80

Existen procedimientos formales para la administración de la evidencia digital



	2008	2009	2010
No	51,50	50,94	29,91
Si	30,90	33,96	23,36
No Sabe	17,60	15,09	7,48
Existen algunos procedimiento informales	-	-	39,25

Comentarios generales:

Si bien este año se muestra un leve decremento en la conciencia de la evidencia digital, aún se refleja la preocupación por el tratamiento de los incidentes que se presentan en temas de seguridad de la información. Lo que muestran los segundos resultados es que si bien nos preocupamos por atender los incidentes y la intención de tratarlos, no tenemos claros los procedimientos formalmente definidos dentro de las organizaciones para poder tener una consistencia en caso de ser requeridos ante un ente judicial, lo que indica es que debemos preocuparnos por mejorar las prácticas de tratamiento de evidencia digital y volvernos más formales dentro de las empresas, para manejar estos temas y tener consistencia frente a los entes judiciales, si es que ese fuere el caso.

Herramientas y prácticas de seguridad

Número de pruebas de seguridad realizadas

	2008	2009	2010
Una al año	28,02	27,84	42,04
Entre 2 y 4 al año	29,67	27,32	23,40
Más de 4 al año	10,99	8,76	4,26
Ninguna	31,32	36,08	30,32

Comentarios generales:

Los resultados de esta sección poseen pocas variaciones frente al año anterior. Por un lado, un grueso de la población adelanta al menos una prueba anual y se mantiene como tendencia en los últimos años, mientras el 30% no hace ningún esfuerzo en este sentido. Así mismo, en comparación con otros años ha disminuido la tendencia a evaluar las infraestructuras de TI de las organizaciones y que una prueba al año, muestra la realidad de las infraestructuras. Estas cifras deben llevarnos a meditar en la inseguridad de la información y sobre las posibilidades que los intrusos pueden materializar para realizar sus acciones. Las pruebas no van a agotar la imaginación que tienen los atacantes para vulnerar nuestras infraestructuras, pero si nos dan un panorama de lo que pueden hacer, nos ayudan a evitar el síndrome de la "falsa sensación de seguridad". No hacerlo es arriesgarse a ser parte formal de las estadísticas de aquellos para quienes la seguridad es sólo un referente tecnológico.

Mecanismos de Seguridad

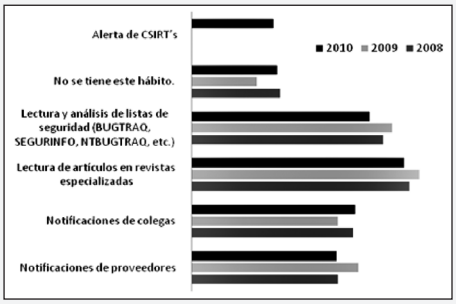
Continúa

	2008	2009	2010
Smart Cards	11,3	13,9	12,62
Biométricos (huella digital, iris, etc.)	19,7	16,0	29,44
Antivirus	76,4	77,8	83,18
Contraseñas	78,3	75,8	79,44
Cifrado de datos	42,9	41,2	42,06
Filtro de paquetes	28,1	30,9	27,10
Firewalls Hardware	49,3	55,7	62,62
Firewalls Software	58,1	52,6	55,61
Firmas digitales/certificados digitales	27,6	34,5	35,98
VPN/IPSec	51,2	54,1	51,87
Proxies	54,2	44,8	48,60
Sistemas de detección de intrusos	27,1	30,9	30,84
Monitoreo 7x24	22,7	19,1	23,83
Sistemas de prevención de intrusos	20,7	27,3	28,97
Sistemas de detección de anomalías - ADS	4,93	7,2	4,21
Firewalls de aplicaciones web - WAF	22,2	21,6	17,29
Administración de Logs	26.6	26,3	26,64
Herramientas de validación de cumplimiento con regulaciones internacionales	8,8	7,2	7,01
Monitoreo de Bases de Datos	-	23,7	28,04
Otro, especifique: antispyware, antispam, honeypots, inForce, monitoreos transaccionales	-	3,1	2,34

Comentarios generales:

Esta sección muestra los antivirus, contraseñas, firewalls de hardware, sistemas de detección y prevención de intrusiones dentro de las más importantes herramientas utilizadas y un alza importante en los sistemas de firmas digitales o certificados digitales. Uno de los datos importantes es el creciente uso de los mecanismos de biometría en el ambiente de negocio, como una barrera más en la protección de la información; se observa un decrecimiento en la utilización de las tecnologías de firewalls de aplicaciones, que contrasta con el crecimiento en disponer de firewall de bases de datos. Así mismo se observa que las empresas están gastando un poco más en mejorar la calidad del software que compran a terceros, o que producen y que mejoran los mecanismos de protección, en cuanto al acceso de los datos.

¿Cómo se entera de las fallas de seguridad?



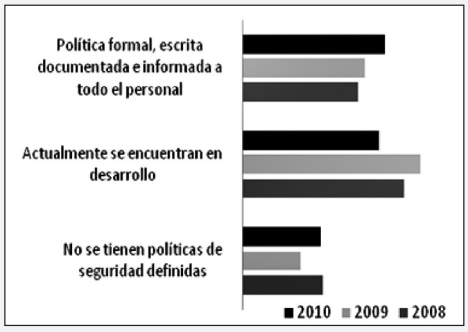
	2008	2009	2010
Notificaciones de proveedores	33,49	38,1	33,18
Notificaciones de colegas	36,94	33,5	37,38
Lectura de artículos en revistas especializadas	49,75	52,1	48,60
Lectura y análisis de listas de seguridad (BUGTRAQ, SEGURINFO, NTBUGTRAQ, etc.)	43,84	45,9	40,65
No se tiene este hábito.	20,19	14,9	19,63
Alerta de CSIRT's	-	-	18,69

Comentarios generales:

Este año vemos cómo se han desmejorados los vínculos entre las empresas prestadoras de servicios de seguridad y las organizaciones, dado que muestran un decremento importante a la hora de notificación de las fallas de seguridad. Por otra parte, hay una mejoría en la confianza con los colegas y/o la comunidad alrededor de la seguridad de la información, frente a los años anteriores, resaltando que los usuarios encuestados dicen dedicarle más tiempo a listas de seguridad como SEGURINFO. La lista de seguridad continúa creciendo, con 2000 participantes en este momento, desde su fundación en el año 2000. Una nueva categoría incluida es la comunicación con distintos CSIRT's que presenta unos datos importantes. También hay relación con los centros de atención de Latinoamérica cuando de incidentes se habla; eso también se ve reflejado con la realidad internacional, la cual refleja una interacción mayor entre estos centros especializados en estudiar las anomalías, y los sectores que se ven involucrados.

Políticas de seguridad

Estado actual de las políticas de seguridad

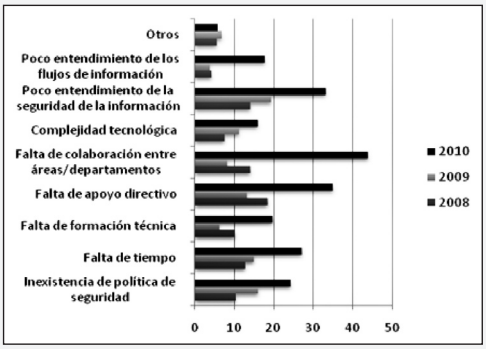


	2008	2009	2010
No se tienen políticas de seguridad definidas	22,53	16,15	21,86
Actualmente se encuentran en desarrollo	45,05	49,69	38,25
Política formal, escrita documentada e informada a todo el personal	32,42	34,16	39,89

Comentarios generales:

Este año alrededor del 60% de las empresas en Colombia o bien no cuentan con política de seguridad definida formalmente o se encuentran en desarrollo. Hay que resaltar un aumento en 5 puntos en el porcentaje de crecimiento de aquellas organizaciones que dedicaron atender esta gran recomendación que enmarca a las organizaciones dentro del contexto de la protección, como un escenario con incidencia en las estrategias de los negocios. Si bien estas cifras muestran que se ha avanzando en temas de tecnologías de seguridad de la información, las políticas de seguridad aún requieren un esfuerzo adicional conjunto entre el área de negocio y la de tecnología. La seguridad de la información por reacción y como apoyo a las funciones de negocio, es más costosa en el largo plazo; mientras una función de seguridad articulada con las estrategias de negocio y vinculada a la visión de los clientes, puede generar mucho más valor y asimilar mejor las fallas de seguridad que se presenten.

Principal obstáculo para desarrollar una adecuada seguridad



	2008	2009	2010
Inexistencia de política de seguridad	10,40	16,15	24,30
Falta de tiempo	12,70	15,00	27,10
Falta de formación técnica	10,10	6,25	19,63
Falta de apoyo directivo	18,50	13,13	35,05
Falta de colaboración entre áreas/departamentos	14,00	8,13	43,93
Complejidad tecnológica	7,50	11,25	15,89
Poco entendimiento de la seguridad de la información	14,00	19,38	33,18
Poco entendimiento de los flujos de información	4,20	3,75	17,76
Otro: Asignación presupuestal, falta de recurso humano, cultura de la empresa	5,50	6,88	5,61

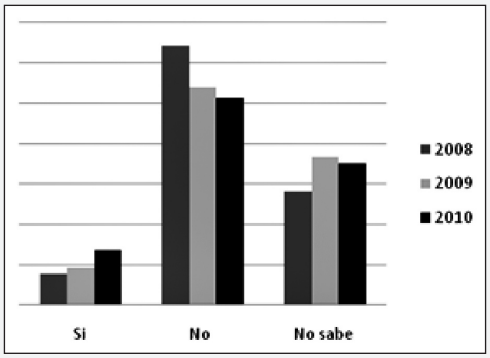
Comentarios generales:

Este año un elevado porcentaje de los encuestados contestó que no existe colaboración entre las diferentes áreas o departamentos de la organización, la falta de sinergia muestra que aún se ve a la seguridad de la información, como un elemento distante del negocio. Indica una desarticulación entre lo que el negocio presta y lo que realmente le ofrecen estas áreas de seguridad de la información a las organizaciones. Así mismo, se observa un número significativo de encuestados manifestando que sus altas direcciones aún no ven la seguridad de la información como un elemento de apoyo estratégico fundamental, a la hora de la prestación de los servicios. Se refleja también que los responsables de vender

la seguridad dentro de las organizaciones, todavía no han encontrado las estrategias necesarias para entender las necesidades de seguridad de la información personalizable a la organización a la que les prestan los servicios. Una tendencia marcada en los ambientes mundiales, es que se piensa que los modelos se pueden replicar sin el más mínimo esfuerzo de adaptación a las necesidades de las compañías y estos resultados reflejan que esta situación es una realidad latente en las organizaciones. Sigue figurando la falta de tiempo, la inexistencia de una política de seguridad de la información, la complejidad tecnológica.

No entender la seguridad de la información significa no involucrar la seguridad dentro del contexto de negocio; también el poco esfuerzo ejercido por los profesionales para vender la distinción de la seguridad y la necesidad de desarrollar un lenguaje que permita la integración entre el proceso y la protección de la información.

Contactos para seguir intrusos



	2008	2009	2010
Si	7,69	9,32	13,66
No	64,29	54,04	51,37
No sabe	28,02	36,65	34,97

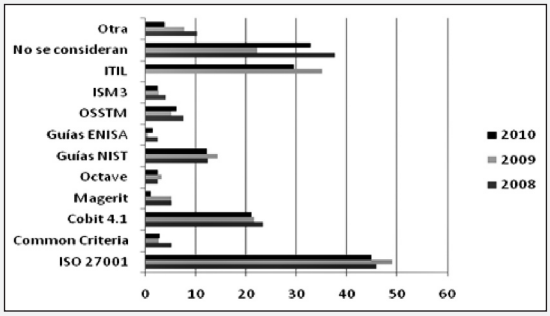
Comentarios generales:

En este año y como escenario clave hay un aumento en denunciar los incidentes de seguridad de la información; ya están más definidos los contactos para trabajar las investigaciones judiciales frente a esos incidentes. Es decir, que la preocupación por seguir los incidentes es importante. Hay que agregar y sobre todo cuando en Colombia existe una legislación al respecto de los delitos informáticos que ha avanzado frente a las amenazas electrónicas, seguir con un proceso de esta naturaleza puede ser más costoso y con pobres resultados.

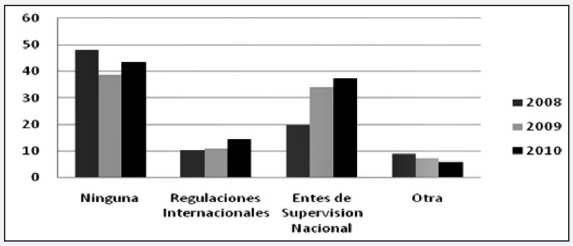
En este punto la academia, los gremios, el gobierno, los proveedores y los usuarios deben organizarse en un frente común para construir estrategias de combate del crimen organizado y en la construcción de modelos de seguridad resistentes a los embates de la inseguridad de la información. Además, establecer acuerdos interinstitucionales con entes de policía judicial para oportunamente frente a una conducta punible en medios informáticos.

Dentro de los más comunes puntos de contacto están DIJIN, el CSIRT de la Policía Nacional, SIJIN y Fiscalía; y, algunos incipientes grupos internos de atención de incidentes.

Estándares y buenas prácticas en seguridad informática y regulaciones en seguridad de la información



Estándar o Buena Práctica	2008	2009	2010
ISO 27001	45,80	49,0	44,86
Common Criteria	5,20	2,6	2,80
Cobit 4.1	23,40	21,6	21,03
Magerit	5,20	5,2	0,93
Octave	2,3	3,1	2,34
Guías NIST	12,30	14,4	12,15
Guías ENISA	2,3	0,5	1,40
OSSTM	7,50	5,2	6,07
ISM3	3,90	2,6	2,34
ITIL	26.90	35,1	29,44
No se consideran	37,70	22,2	32,71
Otra	10,20	7,7	3,74



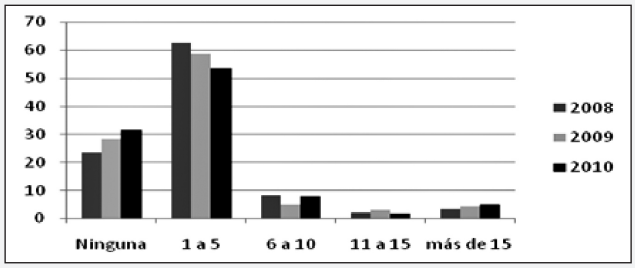
Norma	2008	2009	2010
Ninguna	48,11	38,7	43,46
Regulaciones Internacionales	10,37	10,8	14,49
Entes de Supervisión Nacional	19,81	34,0	37,38
Otra	8,96	7,2	6,07

Comentarios generales:

Esta pregunta indica que para Colombia, ISO/IEC 27001, Cobit, Nist, e ITIL son las prácticas más utilizadas en el área de seguridad de la información usadas dentro de las organizaciones. Utilizar un marco de estos contempla crear procesos metódicos de trabajo con los cuales se pueden construir modelos adecuados de protección de información para las organizaciones. En la segunda sección donde se evalúan las regulaciones aplicables a las organizaciones vemos cómo la normativa de los entes de control nacional (Superfinanciera de Colombia, CRT, entre otros), junto con las regulaciones internacionales como (SOX, BASILEA, entre otros) influye dentro de la población. Un gran número de encuestados dice no estar cubierto por ninguna de las propuestas, mostrando que los esfuerzos en seguridad de la información son parciales y sectorizados, lo que implica la necesidad de una dinámica similar a la de la Banca, para generar un esfuerzo común en procura de una cultura de seguridad de la información más homogénea y dinámica.

Capital intelectual

Número de personas dedicadas a seguridad informática

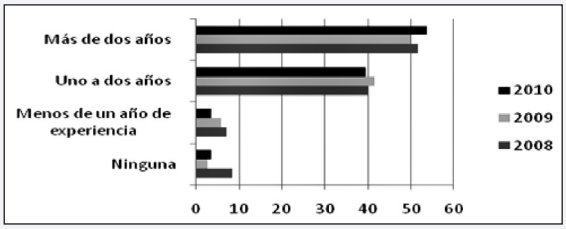


	2008	2009	2010
Ninguna	23,65	28,21	31,64
1 a 5	62,56	58,97	53,67
6 a 10	8,37	5,13	7,91
11 a 15	1,97	3,21	1,69
más de 15	3,45	4,49	5,08

Comentarios generales:

Los resultados de este año nos muestran una leve disminución en la población de personal dedicado (1 a 5), pero muestran leves aumentos en otras franjas (6 a 10, 11 a 15 y más de 15). Tales resultados indican que las grandes empresas están preocupadas por dedicar más recursos en el tema de seguridad de la información, dado las exigencias internacionales o de regulaciones nacionales que les apliquen. No deja de preocupar el 31,64%, el cual representa un incremento frente al año anterior de 3,43%, que no tiene ninguna persona dedicada exclusivamente al tema de seguridad, lo que sugiere que existe una porción importante de empresas que todavía no dedican formalmente recursos a este asunto.

Años de experiencia requeridos para trabajar en seguridad informática

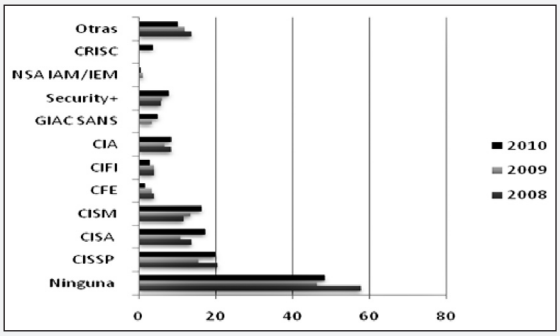


	2008	2009	2010
Ninguna	8,39	2,56	3,39
Menos de un año de experiencia	7,1	5,77	3,39
Uno a dos años	39,9	41,67	39,55
Más de dos años	51,61	50,00	53,67

Comentarios generales:

La tendencia de estos tres años nos muestra que es necesario para las empresas colombianas poseer recursos con experiencia entre uno a dos años, como base para trabajar en los temas de seguridad de la información. El 2011 nos muestra que el 92% de los encuestados consideran importante la experiencia de las personas dedicadas a la seguridad de la información. Cada vez menos personas consideran que los recursos humanos dedicados a la seguridad de la información no deben tener experiencia en esta rama.

Certificaciones en seguridad informática

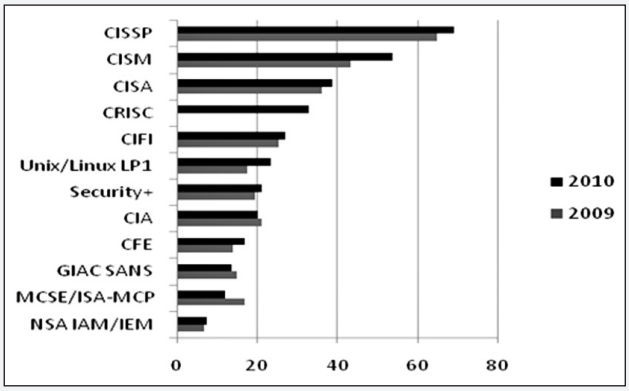


	2008	2009	2010
Ninguna	57,90	46,4	48,60
CISSP	20,50	15,5	20,09
CISA	13,80	10,8	17,29
CISM	11,80	13,4	16,36
CFE	4,0	3,6	1,87
CIFI	4,0	4,1	2,80
CIA	8,40	6,7	8,41
GIAC SANS	-	3,6	5,14
Security+	5,91	6,2	7,94
NSA IAM/IEM	-	1,0	0,47
Otras: Especializaciones en Auditoría de Sistemas, Especializaciones en Seguridad Informática, Diplomados en Seguridad Informática, Auditor Líder BS7799, Certified Ethical Hacking, CCNA, CCSP, GSEC, MCSE, etc.	13,8	11,9	10,28

Comentarios generales:

En este año vemos un aumento moderada en el personal que dice no contar con certificaciones de seguridad de la información. Aumento importante en la certificación CISSP, CISA, y CISM, certificaciones orientadas a los temas de gerencia de la seguridad de la información. Esto resultados reiteran el llamado a la academia para atender la demanda de formación en estas áreas, que actualmente las organizaciones exigen como un nuevo perfil para fortalecer sus esquemas de seguridad y control de cara a la exigencia de un escenario globalizado. Dentro del grupo de las otras certificaciones se resalta que algunos encuestados hablaron de CEH, como una certificación importante a la hora de trabajos con la seguridad de la información, en este sentido lo que se está buscando son especialistas certificados en ethical hacking, que es una tendencia local en aumento que requiere especialistas formados en la materia.

Importancia de contar con certificaciones en seguridad informática

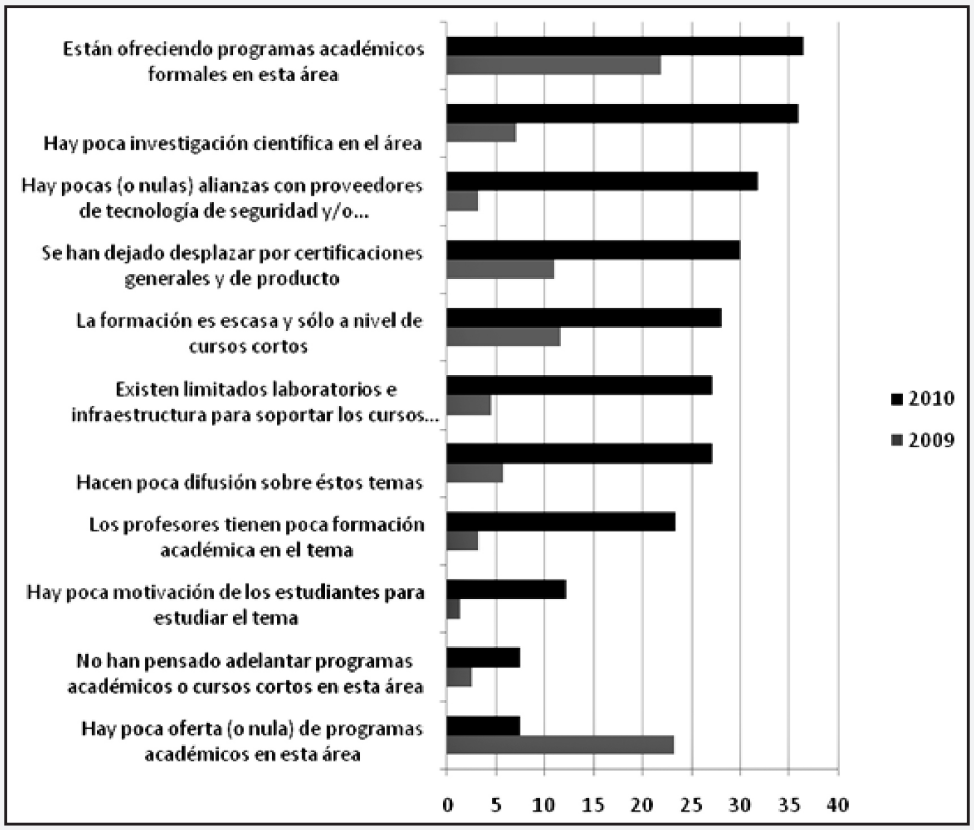


	2009	2010
CISSP	64,9	69,16
CISA	36,1	38,79
CISM	43,3	53,74
CFE	13,9	16,82
CIFI	25,3	27,10
CIA	21,1	20,09
GIAC SANS	14,9	13,55
MCSE/ISA-MCP	17,0	12,15
Unix/Linux LP1	17,5	23,36
Security+	19,6	21,03
NSA IAM/IEM	6,7	7,48
CRISC	-	32,71

Comentarios generales:

Las respuestas de los encuestados nos muestran las certificaciones CISSP, CISM y CISA, así como la nueva CRISC. Son las más valoradas por el mercado y las que a la hora de considerar un proyecto de seguridad de la información marcan la diferencia para su desarrollo y contratación. Otras certificaciones como CFE, CIFI y LPI también reflejan algún grado de importancia dentro del plus que los especialistas en seguridad con formación académica pueden obtener. Se debe resaltar que las certificaciones son referentes para la industria, frente a las tendencias internacionales, pero es necesario fortalecer la formación académica formal en los temas de seguridad, control y auditoría, así como las áreas de manejo de fraude, como una estrategia complementaria en el esquema de certificaciones.

Papel de la Educación Superior en la formación de profesionales de seguridad de la información



	2009	2010
Hay poca oferta (o nula) de programas académicos en esta área	23,23	7,48
Están ofreciendo programas académicos formales en esta área	21,94	36,45
La formación es escasa y sólo a nivel de cursos cortos	11,61	28,04
Se han dejado desplazar por certificaciones generales y de producto	10,97	29,91
Hay poca investigación científica en el área	7,10	35,98
Hacen poca difusión sobre éstos temas	5,81	27,10
Existen limitados laboratorios e infraestructura para soportar los cursos especializados	4,52	27,10
Los profesores tienen poca formación académica en el tema	3,23	23,36
Hay pocas (o nulas) alianzas con proveedores de tecnología de seguridad y/o agremiaciones relacionadas con el tema	3,23	31,78
No han pensado adelantar programas académicos o cursos cortos en esta área	2,58	7,48
Hay poca motivación de los estudiantes para estudiar el tema	1,29	12,15

Comentarios generales:

Los datos este año arrojan resultados interesantes. Por una parte, un 36,45% considera que las ofertas de programas académicos al respecto de los temas de seguridad de la información, cumplen con sus expectativas; sólo un porcentaje de 7,48% piensa que no existen programas o ofertas académicas en estos asuntos, en comparación con el año anterior, que fue de un 23%,. Este año un 28,04% cree que no es suficiente con ofrecer programas cortos en materia de seguridad de la información, y un 29,91% piensa que, si bien es cierto que las certificaciones son importantes, se observa que este tipo de formación no formal, está reemplazando las propuestas académicas realizadas por las diferentes instituciones del país. Además, los encuestados resaltan la importancia de hacer más difusión de sus programas en procura del conocimiento de la comunidad nacional de estudiantes que desean pensar en la opción de una preparación postuniversitaria. De la misma manera enfatizan en el hecho de que existen pocas o nulas relaciones con los proveedores de tecnologías de seguridad. Un tema nuevo que se incluyó para este año fue la formación de los profesores y se manifiesta que aunque existen, no están preparados frente a las expectativas de los estudiantes que son quienes evalúan su conocimiento.

Conclusiones generales

Los resultados generales que sugiere la encuesta podríamos resumirlos en algunas breves reflexiones:

1. Son motivadores de la inversión en seguridad: la continuidad de negocio, el cumplimiento de regulaciones y normativas internas y externas, así como la protección de la reputación de la empresa.

2. Las regulaciones nacionales e internacionales llevarán a las organizaciones en Colombia a fortalecer los sistemas de gestión de la seguridad de la información. Actualmente, la norma de la Superfinanciera comienza a cambiar el panorama de la seguridad de la información en la Banca y en el país.

3. La industria en Colombia exige más de dos años de experiencia en seguridad informática, como requisito para optar por una posición en esta área. De igual forma, se nota que poco a poco el mercado de especialistas en seguridad de la información toma fuerza, pero todavía la oferta de programas académicos formales se encuentra limitada, lo que hace que las organizaciones opten por contratar a profesionales con poca experiencia en seguridad para formarlos localmente.

4. Las certificaciones CISSP, CISA, CISM y CRISC son la más valoradas por el mercado y las que a la hora de considerar un proyecto de seguridad de la información marcan la diferencia, para su desarrollo y contratación.

5. Las cifras siguen mostrando los mecanismos tradicionales de protección

como los antivirus, las contraseñas, los firewalls de software y hardware como los mecanismos de seguridad más utilizados, seguidos por los sistemas VPN y proxies, así como un aumento creciente en el uso de certificados digitales. Existe un marcado interés por las herramientas de cifrado de datos y los firewalls de bases de datos que establecen dos tendencias emergentes, ante las frecuentes fugas de información y migración de las aplicaciones web al contexto de servicios o *web services*, así como la biometría como mecanismo alterno de protección de la información

6. Frente a las amenazas electrónicas, se nota una focalización o centralización de los ataques informáticos; pasamos de virus genéricos, a ataques dirigidos y con objetivo, que disminuyen en su capacidad de replicación, pero aumentan en su efecto organizacional.

7. Se nota que en la realidad nacional se ha realizado un esfuerzo alrededor de la gestión de los incidentes, sin decir que estamos bien, el esfuerzo por entender este escenario como parte fundamental del modelo de seguridad de la información de la organización, indica una mejoría significativa en la gestión de la seguridad de la información, igual que la relaciones que se han venido fortaleciendo con los entes judiciales; son esfuerzos logrados por los diferentes tipos de industrias, en procura del mejoramiento.

8. Aunque existe una legislación en temas de delito informático en el país, llevar a cabo un proceso jurídico puede resultar costoso.

9. Los sistemas de gestión de seguridad de la información demandan de las organizaciones mayores esfuerzos, los cuales parten desde las políticas de seguridad de la información, uno de los talones de Aquiles de los procesos de seguridad de la información de las organizaciones.

10. Los estándares internacionales de la industria se ven reflejados en Colombia en el tema de las buenas prácticas en seguridad de la información; es por eso que el ISO 27000, el Cobit 4.1 y las Guías del NIST son bastante aceptados en los departamentos de tecnología informática.

11. La inversión en seguridad de la información se encuentra concentrada todavía en tecnología (las redes y sus componentes, entre otros), así como la protección de datos de los clientes y un ligero interés en el tema de control de la propiedad intelectual y derechos de autor.

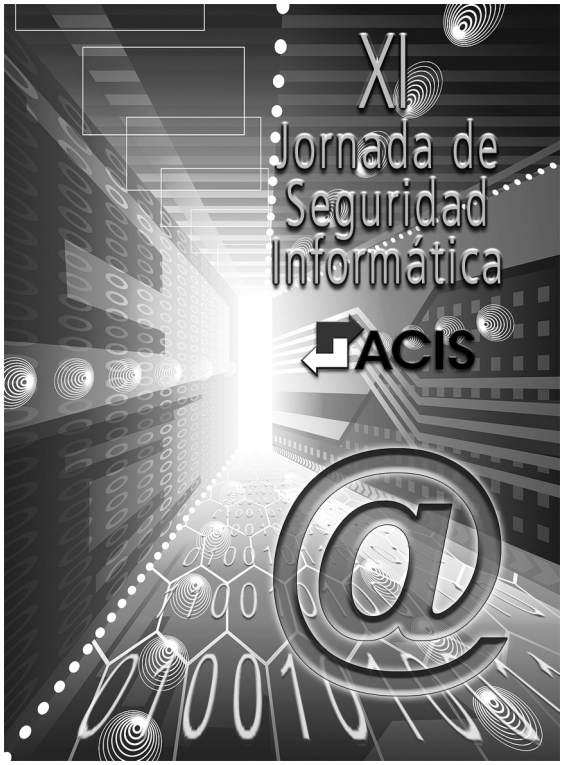
Referencias

[1] PRICEWATERHOUSECOOPERS (2010). The Global State of Information Security Study. http://www.pwc.com/gx/en/information-security-survey/pdf/giss-2011-survey-report.pdf

[2] Deloitte (2011). The Future of Security. http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/AERS/us_aers_future_of_security_01142010.pdf

Notas al pie de Página

[1] Agradecimientos especiales al Ph.D Jeimy José Cano por su apoyo y para contar con la revisión de nivel conceptual de la encuesta. Así mismo, la disposición y oportunidad del Ing. Luis Mauricio González Motavita, para adelantar con oportunidad y efectividad la encuesta nacional de seguridad informática.



Andrés Ricardo Almanza Junco, M.Sc. ITILv3. *Ingeniero de Sistemas, Universidad Católica de Colombia. Especialista en Seguridad de Redes de la Universidad Católica de Colombia. Magíster de Seguridad Informática de la Universidad Oberta de Cataluña, España. Certificación LPIC1, Linux Professional Institute. ITILv3. Codirector de las Jornada Nacional de Seguridad Informática. Coordinador Colombia de la Encuesta Nacional de Seguridad Informática. Oficial de Seguridad de la Información de la Cámara de Comercio de Bogotá.*

Fuga de información ¿amenaza real?

Sara Gallardo M.

¿Es un asunto potenciado por las personas, los procedimientos, la tecnología?

María Conchita Jaimes

Sergio Pérez B.

Juan Pablo Páez S.

Fredy Bautista G.

Francisco Rueda F.

Jeimy J. Cano

Este hecho sumado a los realizados por atacantes informáticos, para quienes no es difícil sobrepasar protocolos y distintas alternativas tecnológicas de seguridad, hacen de la información un arma estratégica que debe generar alertas en los sectores público y privado.

Ante la magnitud de la problemática, la revista reunió a varios especialistas en estos asuntos, para mirar desde las dos instancias, los requerimientos, las carencias, el entorno jurídico y otros aspectos relacionados con la información como activo fundamental del Estado y del ambiente empresarial en el país.

Fredy Bautista García, jefe Área de Investigaciones Tecnológicas de la Policía Nacional; Sergio Pérez Barrera, coordinador de Controles Técnicos del Departamen-

to Administrativo de Seguridad (DAS); Juan Pablo Páez S., Security Arquitect Manager de Etek International; y, María Conchita Jaimes, directora ejecutiva de Ernst & Young dieron respuesta a las inquietudes planteadas durante el debate.

Jeimy J. Cano
Moderador del foro

Antes de formular las inquietudes que rodearán el debate, es oportuno contextualizar el ambiente que rodea a la fuga de información. Hoy vamos a tratar un tema que todo el mundo sabe que existe, pero al que nadie se refiere. Un informe consultado del Grupo Paradell del 2009[1] muestra que los canales más utilizados para ello son correo electrónico (47%), dispositivos USB (28%), CD/DVD (13%), impresora (5%) y otros medios como FTP, P2P, etc. (7%). La constante indica que todos los comportamientos y prácticas de seguridad asociadas con el tema, tienen que ver con el recurso humano.

Según su experiencia, en Colombia ¿cuáles son los elementos que potencian la fuga de información en las organizaciones? ¿Es un tema de personas? ¿Es un tema de procedimientos? ¿Es un tema de tecnología?

María Conchita Jaimes
Directora Ejecutiva
Ernst & Young

La fuga de información se asocia con los tres elementos señalados en la pregunta: personas, procedimientos y tecnología. Y aunque todos están unidos e interactúan de forma coordinada, la fuga de información se da primariamente por personas, impactando los procedimientos y la tecnología.

Francisco Rueda
Director Revista Sistemas

De acuerdo con esa respuesta, ¿cuál es la parte débil? ¿los procesos?, ¿es descuidada la tecnología?, ¿las personas son muy informales?

María Conchita Jaimes

En mi concepto, todo radica en una falta de gobierno y de orientación sobre la administración de la información en una compañía. De ahí nace todo, porque depende de la alta gerencia el esquema de gobierno. Los procesos y la tecnología son asuntos muy operativos que no siempre dependen de la estructura táctica y/o estratégica. Si en una organización no existe un adecuado gobierno con foco de cultura de control y de administración de riesgos, ni la tecnología ni los procesos van a funcionar de manera acorde, porque no se encuentran dentro de ese lineamiento corporativo. Pienso que de los tres elementos planteados, el foco primario es el tema estructural que nace en una estructura de gobierno.

Sergio Pérez B.
Coordinador Controles Técnicos
DAS

A nivel de la investigación criminal y considerando el tema reactivo, es decir, después de sucedidos los hechos, se pueden determinar como causantes de la fuga de información, fallas sistémicas de la organización, en lo que tiene que ver con las personas; con fallas en los procesos y con debilidades en la tecnología, dependiendo de la naturaleza de la fuga. Porque muy probablemente hay fugas de información de carácter interno dentro de la organización o eventos

relacionados con ataques o intrusiones externas teniendo en cuenta las vulnerabilidades de la organización, lo cual ocasiona la fuga. De hecho, es una cadena que involucra en los diferentes casos, los tres temas. Estas situaciones se pueden comparar con temas y aspectos que influyen para la comisión de delitos informáticos, dependen de la motivación y otros aspectos directamente relacionados con las personas. Si son económicos son muy difíciles de manejar, a pesar de que se disponga de suficientes controles. Si son procedimentales o tecnológicos es porque no existen mecanismos de control para mitigarlos o existen fallas en las plataformas que permiten el ingreso y la vulneración de los datos.

Juan Pablo Páez S.
Security Arquitect Manager
Etek International

Es importante tener en cuenta cómo toda la información que va alrededor de la empresa y lo que la hace exitosa dentro del ambiente de negocios es precisamente todo lo informático. Y, al mismo tiempo, cómo las organizaciones están empoderando a la gente sobre el manejo de la información para optimizar y mejorar. En otras palabras, se le ha dado más protagonismo a la información y, por supuesto, a la tecnología como herramienta de desarrollo. En tal sentido, se ha crecido y se ha evolucionado. Pero, en los asuntos de manejo, no se sabe qué es lo importante ni lo confidencial, ni qué lo público. No se ha avanzado en la cultura de saber qué es lo realmente crítico para la organización. Otros estudios muestran estadísticas sobre la fuga de información y señalan que cerca del 80% de los eventos relacionados con la información son producidos por motivaciones sin intención, por no conocer qué pasa; por ignorancia o por aprovechamiento de otras personas que simplemente desconocen el funcionamiento y la importancia de la información, y permiten la fuga de la misma. Otro aspecto es el vengativo, criminal con un propósito negativo. Ahí hay una brecha muy grande para poder trabajar. ¿Cómo hago para educar a la persona que es el motivador, para que sepa qué es lo bueno y lo malo, qué se debe hacer y qué no? Teniendo claridad al respecto, entonces saldrán los procedimientos, la tecnología para moldear la organización, teniendo en cuenta aspectos tales como gobierno y riesgo para mitigar las amenazas.

Fredy Bautista G.
Jefe Área Investigaciones Tecnológicas
Policía Nacional

Existe mucha información en las organizaciones impactada por la tecnología. Hay muchos procesos que antiguamente se hacían en el papel, otros que han sido sistematizados y esa información que se ha almacenado digitalmente es mucho más vulnerable que la existente en papel. Eso es indudable. La tecnología permite tener la información al alcance de un clic. Las personas también forman parte de las causas. Hay una pérdida de valores, falta de ética, de moral, causas que nosotros encontramos en las investigaciones. En ocasiones, soy muy escéptico cuando inicio alguna, porque pienso si realmente se está fugando la información o si fue un error humano. Pero, lo que hemos encontrado es que existe el negocio de la fuga de información. Lo último que hemos descubierto muestra personas que se dedican a traficar con la información, que buscan permear las organizaciones. Es un problema grave, de personas sin valores que sustraen información para comercializarla, personas que almacenan

y guardan información. Basta mencionar el reciente caso de la salud con sendas bases de datos. Me gusta ser escéptico, esperar poco para encontrar mucho. Y en el caso citado es mucho lo que se ha encontrado. Para resumir, la fuga sí obedece a una suma de varios elementos: la existencia de información almacenada digitalmente, que basta copiarla lo cual se facilita mucho. De igual manera, nos preocupamos mucho por la tecnología, pero dejamos de lado la ética y los valores, por parte de quienes pueden tener acceso a la información en procesos sensibles. En tal sentido, el tema económico es clave, y la corrupción juega un papel fundamental. Vale la pena revisar con detenimiento cómo cerrarle el paso y cómo crear conciencia sobre los valores perdidos. En ese entorno encontramos los perfiles de quienes han tenido que ver con la fuga de información, y encontramos a personas con formación en sistemas que saben cómo administrarla, manejarla y, además, viven del tráfico de la misma.

Francisco Rueda

¿Son personas especializadas en todo el proceso de fuga de información?

Fredy Bautista G.

Sí, se trata de grupos especializados que viven del tráfico y el comercio de la información. Es una economía criminal.

Sergio Pérez B.

Son organizaciones delincuenciales bien estructuradas con tareas específicas. Hay grupos especializados en obtener información en la red, con herramientas para acceder a correos electrónicos, obtener claves, cuentas. Otro nivel se ocupa de la venta de la información, es otro eslabón de la cadena que se presta para la comercialización de la información. Es una industria para traficar con información confidencial.

Sergio Pérez B.

En los diferentes medios de comunicación se encuentran avisos clasificados donde se comercializan datos e información, como por ejemplo, vendo en $500.000 una base de datos y, efectivamente se realizan las transacciones donde hay intermediarios y explícitamente se prestan cuentas bancarias para realizar los correspondientes pagos. En efecto, se compran las bases de datos con información confidencial tanto a nivel personal como información sensible de organizaciones y empresas, las cuales son de carácter reservado y están incurriendo en conductas punibles que llevan a la respectiva judicialización, toda vez que este tipo de actuaciones están tipificadas y son castigadas por nuestro código penal colombiano.

María Conchita Jaimes

La fuga de información tiene unos focos importantes y en las estadísticas que uno encuentra, se registra que ésta se debe en su mayor parte a accidentes que ocurren, de no intencionalidad. Es decir, existen muchos casos que no son detectados por la falta de cultura. Lo otro también es que dos de las personas aquí presentes trabajan en un sector en donde los casos que se ven son muy distintos a los que se ven en el ambiente empresarial. Son dos mundos distintos, cuando hay fuga de información de manera accidental, sucede en ambientes privados, como por sectores de industria. El otro foco ya detectado está en temas de gobierno del Estado, en

donde hay información más amplia. Así que la fuga de información tiene dos frentes muy importantes totalmente distintos que dependen del ámbito donde se estén manejando y sobre el tipo de información de que se trate.

Francisco Rueda

Fredy y Sergio se refieren al sector oficial, pero ¿qué sucede en los demás?

Fredy Bautista G.

En efecto, así es, pero precisamente por eso me refería a mi condición escéptica sobre la fuga de información. De hecho ésta se puede perder en forma accidental.

Sergio Pérez B.

Nosotros también tuvimos un caso de fuga de información que no fue intencional, fue un error involuntario de un funcionario. Equivocadamente envía un correo electrónico a la competencia con una tabla que contemplaba un asunto netamente comercial. Allí no hubo ninguna intencionalidad, pero si uno analiza de ahí hacia atrás en lo judicial, es necesario revisar los procedimientos, las políticas, los controles a nivel técnico, si existen DLP o esa serie de precauciones. En lo judicial un fiscal entra en un interrogatorio con el funcionario de policía judicial y el empleado logra defenderse hasta establecer que no había ninguna intencionalidad, pero sí se materializó la fuga de información.

Jeimy J. Cano

¿Cuáles son los síntomas más relevantes para identificar la existencia de una fuga de información en curso? O ¿solamente se puede actuar de manera posterior a los hechos?

Fredy Bautista G.

Hay comportamientos que permiten detectar si se está fugando la informa-ción, partiendo del hecho que ésta es un modelo de economía criminal, unos actos que producen dinero y ese es su enfoque. De ahí que hoy las organizaciones deben empezar a detectar ese tipo de comportamientos. Por ejemplo, personas que no quieren salir a vacaciones o estando en ellas se acercan a las oficinas, como una manera de considerarse indispensables. Eso es típico. Los sábados, en las noches, en las vacaciones están presentes los funcionarios corruptos y claro eso se detecta después de ocurrido el hecho. Ahí es cuando se presenta la fuga de información ligada al modelo de economía criminal. El cambio de hábitos en las personas también es una manifestación y eso sucede en las organizaciones; nosotros lo vemos cuando un funcionario resulta con casa, carro y "beca", en un país en donde no es tan fácil la adquisición simultánea de tales elementos. Este es un tema que genera debate. También hemos encontrado en los casos ligados con pérdidas de equipos portátiles, discos duros, memorias, otra vía para la fuga de información. Otra posibilidad son las relaciones dentro de las empresas, una de las dos personas involucradas termina sustrayéndole la información a la otra. En un año hemos detectado ya tres casos similares, en donde el tema es particular. Hasta ahí llegan las cosas y se deberían "abrir los ojos" para estar alerta. Y aquí no estamos hablando de situaciones corporativas. En la vida real todo es posible. Para resumir, se trata de los indispensables, los que cambian hábitos, los que crecen económicamente en forma muy

rápida. En las organizaciones muchas veces no se ocupan de ejercer un control interno al respecto, eso no se revisa y son alertas claras. La más sencilla manifestación también es la salida del empleado hacia la competencia o a montar un negocio propio, que también ocurre.

Juan Pablo Páez S.

Infortunadamente, eso es difícil de detectar de acuerdo con mi experiencia. ¿Cómo podemos determinar cuáles síntomas pueden propiciar la fuga de información? Carecemos de los mecanismos para controlar, educar y prevenir. A mí me sucedió con el sector financiero un caso: se vence mi tarjeta de crédito y me llega a la casa en un sobre sellado el plástico con la instrucción de llamar a un call center para activarla. Eso hice y al cabo de cinco días y de una tarjeta que todavía no había usado por ninguna de las vías posibles, recibo un mensaje de texto anunciándome que dicha tarjeta fue usada en una compra en Lima, Perú. Entonces llamé a la entidad financiera, advertí que yo estaba en el país, ellos procedieron a bloquearla y a los tres minutos otra compra por $800.000 pesos. Hice un análisis del hecho: me llega la tarjeta en sobre cerrado que hay que romper, yo sólo activé la tarjeta y nadie la usó, entonces la única posibilidad es que dentro de la entidad financiera alguna persona lo hubiera hecho. Luego se establece la investigación respectiva. Frente a estos casos esas entidades guardan silencio y sólo se pronuncian si la información sobre el mismo incidente se fuga y se da a conocer al público y entonces se inicia la investigación. Esto es mucho más complejo de determinar y aclarar, porque antes se trataba de una persona que entraba a una oficina, sacaba algo y quedaba registrado en una cámara. Aunque esto todavía sucede, ahora las circunstancias son bien distintas por el avance de la tecnología y la investigación siempre se inicia mucho después de ocurrido el hecho. Entonces la pregunta es: ¿se trata de un terma organizacional o es un asunto tecnológico?

María Conchita Jaimes

Me parece que la identificación proactiva de la fuga de información en Colombia, todavía está en condiciones muy empíricas. Lo que comenta Fredy, por ejemplo, es muy valioso en la medida en que se observan los cambios de comportamiento de las personas, hábitos de vida y en donde entra en juego la malicia indígena. Pero, debido a que la información es todavía un intangible, no existen los mecanismos más formales o estándares propios para crear y establecer la fuga de información. Por lo general, los hechos se descubren después de ocurridos. Hoy en día estamos en un mundo donde no existen fronteras, la información se maneja en cualquier país y a través de dispositivos móviles de todo tipo. Entonces, la información está en todas partes y es muy difícil detectar los hechos que rodean su fuga. Especialmente en los dispositivos móviles o en el ciberespacio es muy difícil detectar cómo se está realizando el manejo de la información, a menos que se tenga establecida una cultura sobre seguridad, para ejercer el control sobre quienes la manejan, pero esto es muy complicado.

Juan Pablo Páez S.

Y en algunos casos relacionados con la información, se está frente a una pantalla de un computador con un balance al frente, ¿cómo se hace para protegerlo de la toma de una fotografía, por ejemplo? La tecnología va mucho más atrás y esto

Jeimy J. Cano (derecha), enfatizó sobre la importancia que las organizaciones deben dar a la fuga de información.

es un tema más cultural de la organización. Para evitar la fuga de información no se trata de disponer de una solución o de un producto, en la medida en que no es posible tapar todo con una mano y las vías de acceso son muchas y muy variadas.

Fredy Bautista G.

En tal sentido existe algo todavía más grave. Si no hemos podido aún con la fuga de información que no involucra tecnología o que no involucra hackers informáticos, ¿qué haremos cuando se presenten los ataques informáticos o accesos abusivos para sustraer información y se masifiquen, considerando que esa es la tendencia? Si no hemos podido aún con la fuga de información física que no contempla ningún aspecto tecnológico, ¿qué haremos en otras circunstancias? La impresora, por ejemplo, que queda en cola con lo que se deja por fuera de un escritorio, con la pérdida de todo lo que se puede cargar en un dispositivo móvil.

Si el tema es complejo aún, ¿se imaginan el panorama cuando se masifique el acceso a un sistema y sea el común de las conductas?

Francisco Rueda

Y ¿existe claramente una tendencia hacia al crecimiento de tales prácticas? ¿Qué se ha podido observar, por ejemplo, durante los últimos cinco años?

Juan Pablo Páez S.

Lo que sucede es que el valor de la información en este momento ha cambiado. Y eso se observa en casos recientes como el de Sony, suscriptores cuya información queda disponible y a la vista. Otra situación como la de RSA.

Sergio Pérez B.

Es como realizar también una analogía por el tipo de empresa en cuanto a su capa-

cidad financiera, de reacción e inversión. Si revisamos por ejemplo la situación de las pymes, ahí vamos a encontrar debilidades en todo sentido. Y en entidades grandes pueden tener los mecanismos de control, de contrainteligencia para lograr que su personal de seguridad pueda estar al tanto de los cambios de comportamientos, de ingresos fuera de los límites normales y, en general, todas las maneras de actuar por fuera de un patrón normal. Y aún así, tales empresas también pueden ser víctimas de fuga de información. Así las cosas el panorama es bien complejo y la tendencia apunta a la obtención de manera ilícita de grandes bases de datos, además de información sensible y privilegiada.

María Conchita Jaimes

Cuando se indaga sobre los síntomas más relevantes si yo como consultora llego a una corporación donde veo que no hay un gobierno ni cultura de control, donde todo el mundo maneja información como quiere, y no hay unos procesos de clasificación de la información, voy muy seguramente a encontrar fuga de información, sea o no intencional. Porque esa carencia lleva a que las personas utilicen la información de acuerdo con su visión particular al respecto. Cada quien le pone el criterio como le parece. Y si faltan estos elementos claves para controlar la fuga de información, siempre existirá el síntoma de que algo se está perdiendo porque los controles no se están dando. ¿Quién educa a quién en el manejo de la información?

Francisco Rueda

Y ¿eso sucede en la mayoría de las empresas? ¿Adolecen de una cultura para asumir el manejo de la información? De ser así, esa es gran parte de la problemática, son muy informales, no les preocupa. No son conscientes del riesgo.

Sergio Pérez B.

Básicamente, la fuga de información es la consecuencia de varias cosas. Primero, se trata de utilizar la información obtenida como medio para la realización de otras conductas como traficar con la información, compra y venta de la misma, para cometer suplantaciones de identidad, como insumo de ingeniería social, para la realización de ataques informáticos, entre otras. Como segundo punto es importante resaltar que si existen incidentes en este tema, es un indicador que para la organización debe generar los mecanismos de alerta y disparar las alarmas correspondientes, toda vez que algo anormal está sucediendo. Es decir, no hay procedimientos, ni controles bien definidos y establecidos, lo cual se debe revisar y generar la respectiva retroalimentación y ajuste en los procesos.

Juan Pablo Páez S.

Entonces en una empresa donde no existe gobierno ni ningún sistema de control, la pregunta es: ¿si sale información y ésta no es relevante para la organización, eso es fuga?

Jeimy J. Cano

Por lo general, la fuga de información a alguien "le duele". Así que una definición podría ser: todas aquellas acciones o actividades que de manera intencional o no permitan el flujo no autorizado de información sensible o crítica fuera de los límites de la organización.

Juan Pablo Páez S.

¿Qué tal que la organización no haya definido sus límites?

María Conchita Jaimes

Si no hay gobierno no hay cultura y, por lo tanto la fuga de información es más probable.

Jeimy J. Cano

Considerando el escenario donde la fuga se materializa, ¿cómo se debe actuar para atender una fuga de información? ¿Existe un procedimiento estándar? ¿Cuáles son los pasos a seguir? ¿En qué no nos podemos equivocar? ¿Cómo proceder?

Fredy Bautista G.

En esa dirección necesariamente debería haber dos ejercicios. Identificar el sitio por dónde se está yendo la información y si involucra un aspecto técnico, debe haber una atención al incidente para identificar la vulnerabilidad y detectar el lugar por dónde se realiza la fuga. Esto contempla un elemento de carácter técnico, informático, pero también la atención del equipo jurídico para atender el incidente. Las organizaciones cada vez deben ser más conscientes de la necesidad de poner a funcionar esos dos escenarios. El que atiende el incidente desde lo informático y quien lo aborda desde el punto de vista jurídico; saber que existe el asunto de la violación del dato, tipificado. Pero desde mi punto de vista las organizaciones deben contemplar tales aspectos para mitigar el impacto del incidente, desde los diferentes ángulos en que puede verse afectada la imagen de la organización y la empresa misma.

Sergio Pérez S.

Debe existir un protocolo de respuesta a incidentes. Ya sea en lo técnico, documental o en la parte física dentro de los procesos de las organizaciones. Un procedimiento permanente de monitoreo que genere las alarmas correspondientes, así como procedimientos explícitos para saber cómo escalar la situación y las acciones correctivas para cada caso, en otros términos gestionar los incidentes de seguridad. Iniciaría básicamente con el manejo de la escena, una primera respuesta a nivel interno de la organización o primer respondiente, y luego con todo el engranaje a nivel procedimental, tanto de protocolos técnico científicos de criminalística y de manejo de campo que requiere el tema, para que en los casos en que esas tipologías se enmarquen en conductas punibles, los elementos materiales probatorios y evidencias físicas no sean refutadas en los procesos judiciales.

María Conchita Jaimes

Mi respuesta contempla dos sentidos. Si la fuga de información fue no intencional tiene que buscarse un procedimiento apropiado para ese caso. Hay que buscar las causas. Si no fue intencional recurro al gobierno y a los procedimientos, porque éste es el que maneja todo. Es necesario revisar cómo funciona el gobierno para saber cómo se ha educado a los empleados, a los asociados para que tales fugas de información no intencionales no se repitan. Si, por el contrario, la fuga de información fue intencional y se dispone de parámetros establecidos y políticas establecidas, vendrá el pro-

cedimiento legal, jurídico, técnico, de entendimiento, forense. Es decir, todos los asuntos asociados a una gobernabilidad con cumplimiento. Y como son dos parámetros diferentes, es necesario disponer de los elementos relacionados que permitan actuar y determinar el incidente y las responsabilidades. Ahora bien, cuando la fuga no es intencional no recae en elementos legales ni jurídicos, sino un asunto que recae sobre la estructura interna de la organización que debe ser revisado.

Sergio Pérez S.

Si se trata de un incidente no intencional lo que genera es una retroalimentación para poner en marcha unos correctivos y remodelar.

Francisco Rueda

Y ¿cómo se determina si el hecho fue voluntario o involuntario?

Fredy Bautista G.

Puede ocurrir algo con el tema de no tomar acciones legales. Y si más adelante esa fuga no intencional trae un riesgo legal se va a cuestionar a la empresa sobre el porqué no hubo denuncia sobre la pérdida de información.

Sergio Pérez S.

En una fuga de información los más afectados son las mismas personas que figuran con los datos sensibles permeados. En el caso de una entidad financiera con una vulnerabilidad en sus bases de datos, por imagen no hay judicialización del caso, y el perjudicado es el usuario, cuyos datos están expuestos. Así que vale la pena darle importancia al hecho de si fue o no de manera intencional.

Sara Gallardo M.
Editora Revista Sistemas

¿Cuáles son las claves que determinan la intencionalidad o no intencionalidad del hecho? ¿Cómo se determina?

Fredy Bautista G.

Descubierta la fuga de información se deben determinar sus causas. Si se dio por una imprudencia, por desconocimiento o ignorancia. Todo esto se debe catalogar y de ahí que insista en el tema legal. La organización tiene que actuar en esa dirección, porque la información puede quedar suelta y no sabemos el uso que se le vaya a dar ni sus consecuencias. Determinar el dolo es muy complicado.

Juan Pablo Páez S.

Pero vale la pena revisar cómo se acorta la brecha en términos del dolo. Cito el caso de una universidad en Suiza, la inclusión de profesores, estudiantes a toda la red del campus, en donde prima la libertad absoluta, cada uno puede hacer lo que quiera y como quiera. El proceso consiste en la expedición de un carné temporal con derecho a recibir capacitación en políticas y manejo de información y seguridad dentro del campus. Entonces la persona recibe educación al respecto y al final del curso se presenta un examen, se certifica y luego el empleado firma el contrato con esas bases. De esa manera la organización ya puede hacer responsable a la persona de lo que haga con la información, sobre incidentes relacionados con su uso y manejo. En otras palabras, antes de hacer algo, el empleado pregun-

ta el alcance de sus acciones, para evitar incumplir con las normas definidas o provocar hacer un mal uso de la información (incidentes de fuga de información). Se trata pues de un asunto de cultura sobre un esquema claro que contemple reglas y condiciones específicas.

Jeimy J. Cano

Si la fuga inicialmente se detecta y la investigación determina que no fue intencional, pero el incidente hizo que bajara la acción de la empresa en la Bolsa de Valores, entonces aquí comienza un juicio de responsabilidades para el equipo responsable por la información.

Juan Pablo Páez S.

La organización debe asumir esa responsabilidad desde antes, para evitar las consecuencias. De ahí la necesidad de establecer claras responsabilidades y procedimientos, dentro de una cultura que lo garantice.

Sara Gallardo M.

¿Eso significa que la tecnología desbordó el alcance cultural del manejo de la información, considerando que la misma tecnología es la que ha convertido la información en un activo y en un aspecto clave en cualquier ambiente?

Juan Pablo Páez S.

Eso es como decir que antes existían carros que alcanzaban 30 kilómetros por hora y construyeron vías para transitar a esa velocidad. Pero pasó el tiempo y los nuevos carros circulan a 100 o 120 kilómetros por hora. Al conductor no se le enseñó que si va a desarrollar esa velocidad debe tomar las curvas de una u otra forma para evitar un accidente, entonces los carros (herramientas tecnológicas evolucionaron), pero al mismo tiempo los mecanismos de control no evolucionaron para crear las normas y prevenciones para poder manejar ese desarrollo tecnológico. La evolución de la tecnología y las normas para hacer un buen uso de esta o se ha dado en la misma proporción. La tecnología ha evolucionado, pero la madurez de las compañías no lo ha hecho al mismo ritmo. Es una brecha gigante que permite cualquier incidente de pérdida o fuga de información

Jeimy J. Cano

Considerando que la fuga de información es inevitable, ¿cuáles son las recomendaciones claves para limitar su materialización? ¿Qué acciones se deben adelantar al respecto?

María Conchita Jaimes

Controlar la fuga de información es inevitable y se puede mitigar. Los riesgos se mitigan, pero no se eliminan. Entonces se trata de generar buenas prácticas de control sobre la información; de que existe el gobierno corporativo para mitigar tales riesgos. Pero no es posible mitigar los riesgos de fuga de información, pensando en que voy a controlar la tecnología, porque hoy en día ésta no tiene límites. Hoy, los mil empleados de una empresa tienen portátiles, memorias USB, iPhone, celulares, de todo, y no se puede controlar ese universo de dispositivos de información. Lo que sí se puede controlar es la cultura de las personas que manejan los dispositivos. Entonces el tema es cómo orientar y establecer unos

mecanismos y una buena cultura para el manejo apropiado de la información. Hace un par de años, el gerente de nuestra compañía aducía que antes no existía el correo electrónico, y hoy tenemos más de 120 empleados utilizándolo. Así que la pregunta que se hacía era ¿cómo controlarlo?, ¿cómo detectar la fuga de información por esas casillas de correo? La respuesta mía fue cultura, políticas, normas, buenas prácticas que eduquen para el buen manejo de la información, porque es imposible estar detrás de cada quien al respecto.

Sergio Pérez B.

Los sistemas de gestión de seguridad enfocados a la prevención de la fuga de información. Pero, de hecho eso va ligado con la generación de una cultura dentro de las organizaciones para capacitar sobre el manejo de la información. Muchas veces el desgaste de las empresas escribiendo las políticas sobre el uso de todos los elementos relacionados con la tecnología es grande, toda vez que no se socializan adecuadamente. Y si no hay el concurso de los usuarios, no se obtienen resultados proactivos en términos de prevención. Por otra parte, es el compromiso de los directivos de las organizaciones para impulsar procesos que generen un impacto y con tal concientización se obtengan buenos resultados sobre el particular. En resumen, se trata de gestionar permanentemente la seguridad, generar buenas políticas, culturizar la gente, capacitarlos y estar en permanente actualización y concientización sobre la seguridad.

Francisco Rueda

¿Pero qué tanto hace eso una empresa si no le "duele"? A los empleados no les importa, en la medida en que no tienen conciencia del beneficio. El día en que algo suceda, la cosa será distinta. No hay cultura porque no se evidencia la necesidad, porque eso implica esfuerzos, recursos, entre otros aspectos.

Juan Pablo Páez S.

Un reciente informe de Forrester sobre DLP de 2011 se refiere a la evolución de la tecnología en ese entorno. Hace tres años cuando DLP fue el boom, los competidores en el mercado eran muchos y al cabo de ese tiempo se ha abierto una distancia muy grande entre los líderes y los rezagados con tendencia a eliminar esa línea, porque no logran capturar el mer-

Es necesaria una cultura orientada a la protección de la información, señalaron los expertos.

cado. ¿Por qué sucede eso? Existe algo en las organizaciones que no las motiva a implementar soluciones de este tipo y como eso no trae dinero, el desarrollo tecnológico también se ve frenado porque no hay investigación sobre la tecnología de fuga de información. El estudio también se refiere a que la tecnología, que debería ser un elemento fundamental en las organizaciones, se ha vuelto un componente de mejores. Esto ha hecho que tecnológicamente el recorrido sea todavía más lento y que quienes lo adelantan lo hagan dependiendo del sector. La motivación para poder gestionar sistemas de prevención de la fuga de información son: Para el sector financiero el cumplimiento y normatividad; para el sector de la industria la motivación es la protección de propiedad intelectual; para el sector de la salud la motivación es el cumplimiento de regulaciones como lo es en Estados Unidos la regulación HIPPA; para el sector público y entidades de gobierno, la protección de la información no pública. Cuando exista la forma o normatividad que exija el control de la fuga de información o la implementación de mecanismos prevención de fuga de información de forma explícita el manejo de incidentes y responsabilidad legal será distinto. Por ahora, el sector más avanzado en Colombia es el sector financiero, las demás áreas no están cubiertas.

Jeimy J. Cano

Entonces, ¿lo que se puede observar después de sus intervenciones es que se necesita "castigar" para que la seguridad funcione?

Sergio Pérez B.

A medida que se presenta un mayor número de incidentes internos o externos en las organizaciones, y de esta manera se han incrementado el número de regulaciones, lo cual genera que si se incumplen, repercutirá en mayores costos fiscales y judiciales.

Jeimy J. Cano

Una recomendación además del aspecto cultural, que someramente se ha planteado, es que hay que detallar de manera formal la responsabilidad en el manejo de la información a la persona específica. Establecer en qué lugar de la descripción del cargo se advierte el nivel de la información que tiene que manejar y los cuidados que debe tener el empleado. Si esto estuviera en dicha descripción la situación sería distinta. Entonces, debe existir esa delegación de responsabilidad.

Sergio Pérez B.

En diferentes entidades lo que se maneja es a nivel de contrato, acuerdos de confidencialidad, lo cual permite que se tengan herramientas para la toma de decisiones por parte de la administración, de manera que si se presentan incidentes como fuga de información se aplica la normatividad vigente. Pero, en las funciones específicas sobre el manejo de la información generalmente no existe.

Jeimy J. Cano

Por esta razón, los acuerdos de confidencialidad no funcionan como se espera, porque lo hecho, hecho está. El tema de la delegación formal tiene que empezar a pesar. ¿Será que las organizaciones sí están preparadas para un Data Lost Prevention -DLP-? Si no hemos

clasificado la información, ¿será que un DLP es la respuesta? Nos adentramos un poco más.

María Conchita Jaimes

La clasificación de la información ni la prevención para fuga de información están en el personal técnico, ni en la tecnología, está en toda la organización, en la medida en que el flujo de la misma es transversal. Y eso involucra a todas las áreas, todos los niveles, todos los cargos, porque la información fluye y, en consecuencia, la clasificación de la información es la base para dar un primer paso de control. En Colombia ese es un tema que, en su mayor parte, se trabajó por la regulación. Y hay entidades en el sector financiero, no son muchas, que ya han trabajado el tema, pero para llegar a eso nos falta bastante en el país, para que la gente crea en el asunto de la clasificación. Sobre la delegación de la responsabilidad en lo relacionado con la gestión de la seguridad de la información, se establecen ítems en las funciones y los perfiles de los cargos. Y, en la medida en que la información circula en forma transversal por la organización, a veces no se puede personalizar, pero si existen políticas claras de clasificación de la información unidas al tema contractual y con la firma de cumplimiento de las políticas de la organización, de manera indirecta se advierte sobre la clasificación de la información y entonces se establece la responsabilidad sobre su manejo y cuidado. Es un asunto que va más allá del término de confidencialidad.

Juan Pablo Páez S.

Cuando en una compañía desean implementar un proyecto de DLP, se indaga por el objetivo que lo anima, y todos los aspectos relacionados. En ese primer instante y de acuerdo con la respuesta, se les habla con claridad para que no pierdan ni tiempo ni dinero. Si no se tiene claridad de los objetivos del proyecto, este no podrá adelantarse nunca porque no tiene la manera de sustentarse. Lo segundo, que hay que identificar es si cuando el cliente piensa que una solución de este tipo es algo así como colocar un antivirus en un PC, estamos muy equivocados. En este tipo de situaciones aterrizar un proyecto con una solución o una estrategia de DLP es muy complejo. Entonces abordamos estas situaciones haciendo un entendimiento de los objetivos de la organización y el flujo de la información para definir las políticas de DLP y encontrar los controles administrativos, tecnológicos y físicos que permitan hacer el control de la información por todos los canales de salida o fuga de la organización.

Sergio Pérez B.

Volvemos al tema de gobierno de las políticas. Clasificación formal de la información alineada con políticas establecidas en la organización, en cuanto a la implementación de niveles de acceso, perfiles, segregación de funciones, entre otros aspectos.

Juan Pablo Páez S.

Hay que determinar qué es lo confidencial con base en la esencia del negocio. Esto no es lo mismo para un área financiera que para una de ventas, por ejemplo. Y lo otro es el ciclo de vida de la información, porque ésta hoy puede tener un valor y mañana otro y su clasificación es dinámica. Son variables adicionales para ver cómo se puede trabajar.

Jeimy J. Cano

Sobre el ciclo de vida de la información, hoy se observan tres vistas. La vista de la calidad de la información, la vista de gestión documental y la vista de seguridad de la información. Todas tienen ciclos de vida. Si se habla con la persona de gestión documental, se refiere al ciclo de vida del documento. Si se hace lo mismo con el de calidad, se habla de oportunidad, consistencia, integridad y completitud. Finalmente, si habla con el de seguridad de la información, se refiere a confidencialidad, integridad y disponibilidad. Entonces viene la siguiente pregunta, ¿con qué criterio califico la información? Esta situación nos hace un llamado de atención en Colombia: ¿por qué no hay una vista unificada del manejo de la información? ¿Quién es el damnificado del asunto?

Juan Pablo Páez S.

En la actualidad nosotros tenemos tres sistemas de gestión, el de calidad, seguridad y uno de prestación de servicios basados en el estándar ISO 20000, los tres sistemas conviviendo de forma independiente puede ser bastante complejo. Pero, realmente lo que se busca es disponer de un sistema integrado y determinar cuál es la política general que cobija a los tres sistemas para trabajar en forma colaborativa. ¿Cómo a través de un sistema de gestión es posible apoyar un sistema de seguridad o el sistema de clasificación de activos, y cómo a través de eso se presta un servicio con ciertas condiciones? Eso requiere un sistema para que todos aporten y puedan convivir. Así que no hablamos de cada asunto por separado, sino de un sistema integral. De pronto a futuro habrá una nueva normatividad y tendremos que ver la manera de adaptarlo a tales circunstancias, pero sigue siendo el mismo sistema. Pasa lo mismo en la regulación, cuando hay que dar cumplimiento a las nuevas normas. Yo no puedo generar equipos separados para que cada uno funcione en forma separada vigilando cada sistema o el cumplimiento de la regulación. Se trata de una sola matriz para cumplir con todo, al finalizar se busca siempre implementar mejores prácticas. Entonces la solución es integrar todos esos mecanismos y no es fácil. Eso requiere que la organización participe y se comprometa de forma activa.

María Conchita Jaimes

Hay que ir más allá de los sistemas de gestión. Las tendencias tecnológicas han hecho que nosotros crezcamos tecnológicamente como islas, en forma desordenada. Todo eso ha contribuido a que la información no haya sido construida en una forma apropiada. Antes de enfocarnos en el sistema de gestión de la información debemos preocuparnos por la existencia de una arquitectura de la información. Hoy en día se habla de las arquitecturas empresariales y si me devuelvo un poco a la construcción de la base tecnológica, empiezo por entender como está mi arquitectura empresarial y a partir de esto construyo la arquitectura de datos para gestionar de manera integrada la información. Los conceptos de Data Management y Data Analytics hay que digerirlos en primera instancia antes de dar un paso hacia la gestión adecuada de la información.

Jeimy J. Cano

¿Qué impactos jurídicos puede llegar a tener, tanto la empresa como el que materializa la fuga, frente al ordena-

miento legal vigente? ¿Podría catalogarse como delito informático?

Fredy Bautista G.

En el tema jurídico habría dos aspectos para tener en cuenta. El primero si a esa fuga de información no sobreviene una conducta delictiva, diferente al simple hecho de que se pierda la información y el dato como bien jurídico protegido, y eso lo catalogaríamos inicialmente como una violación de datos personales, contemplada en la Ley 1273 de Delitos Informáticos, que se refiere a sustraer, comercializar, divulgar, usar información; y las circunstancias de agravación punitiva endurecen las penas cuando el responsable de la acción u omisión es el administrador de la información. Sin embargo, existe otro bien jurídico que es el del ordenamiento económico y social, la violación de reserva industrial y comercial que paradójicamente resulta menos gravoso que el de violación de datos personales, porque apenas se sanciona con aspectos económicos y en el mejor de los casos con penas que no superan los dos años, no sería entonces una situación complicada para la persona comprometida en hechos de tal naturaleza. Si estamos hablando de la información para protegerla sin que sobrevengan otras conductas punitivas en detrimento de carácter económico, claramente estaríamos sobre una violación de datos que debe ser sobre ficheros o archivos que sean considerados así. Ahí entraría otro debate jurídico sobre si lo que se fue es un dato personal o no, pero ante el escenario de que estemos frente a un archivo de un dato personal sí existe una violación, al sustraerse y utilizarse sin la autorización del titular de esa información, y estaríamos frente a una conducta sancionada con penas que parten desde los cuatro años de prisión. Diferente a los otros hechos que sobrevengan a esa fuga de información.

Francisco Rueda

¿Eso quiere decir que en términos de legislación no estamos muy bien?

Sergio Pérez B

La legislación sí tiene algún tipo de herramientas en ese sentido. Complementando lo que mencionaba Fredy, a nivel privado también hay un bien jurídico, un artículo específico relacionado con la divulgación y empleo de documentos reservados que también es catalogado como conducta punible. El que divulgue un documento sin la debida autorización, esto enmarca concretamente lo relacionado con fuga de datos o fuga de información. Pero también está penalizado como multa. Otro artículo del Código Penal es el espionaje; el que indebidamente divulgue algún tipo de secreto político, económico y militar que ponga en riesgo puede ser la organización, también incurre en un delito así catalogado. Pero, además de todo ello, los funcionarios públicos tenemos unos factores de control bien fuertes y aspectos de agravación punitiva, frente a cualquiera de estas faltas. En cuanto a la revelación de secretos que sean un bien público, también produce unas penas excarcelables, menos de cuatro años. La utilización de asuntos sometidos a reserva está penalizada con multa. La utilización de información privilegiada, según la naturaleza del cargo también contempla penalización. La utilización indebida de información obtenida por el ejercicio de la función pública es penalizada con multas. La Ley de inteligencia, la cual está en curso en el congreso de la República, establece que los delitos

mencionados anteriormente, van a tener un incremento en la penalización, y serán castigados con cárcel entre cinco y ocho años, serán no excarcelables.

Fredy Bautista G.

Para mayor precisión, el que sin estar facultado con provecho propio o de un tercero obtenga compile, sustraiga, venda, intercambie, envíe compre, intercepte, divulgue o modifique entre otros, datos personales, bases de datos o medios semejantes incurrirá en prisión. Pero, sobre lo que quiero llamar la atención aquí es que hay una circunstancia sobre penas accesorias y es que si quien adelanta esta conducta y es el responsable de la administración de esa información se le puede sancionar también por tres años, sin habilitación para el ejercicio de la profesión. Es algo que contempla la legislación colombiana y me parece interesante.

Jeimy J. Cano

Aquí vale la pena señalar que después de tener clasificada la información y esta información esté asociada con el cargo y dicho cargo tenga una responsabilidad por el tratamiento de tal información, si se materializa una fuga por negligencia en el tratamiento de la información, no sólo será penalizado dentro de la organización, sino puede ser judicializado con base en el artículo leído por Fredy, porque la responsabilidad es formal dentro de la organización. Entonces se empiezan a ver elementos de la ley hacia la empresa, útiles en la reflexión.

Fredy Bautista G.

Dice además que si quien comete la conducta lo hace aprovechando la confianza depositada por el poseedor de la información, o por quien tuviere un vínculo contractual con éste.

Sara Gallardo M.

¿Cómo entra en juego la prueba en todo esto, a la hora de la judicialización? En otras palabras, ¿estamos preparados en términos informáticos para hacer efectiva una prueba y poder determinar lo que está planteado en la Ley?

Fredy Bautista G.

Absolutamente sí. Lo que ocurre es lo mismo. Las grandes empresas tienen equipos que recogen procesos, para grandes casos. El problema es cuando vamos en la pirámide a escala invertida; la gran mayoría de organizaciones no tienen tal posibilidad para preservar y proteger la prueba. El antiforense sí lo puede hacer. La herramienta técnica existe, el procedimiento se aplica en Colombia cada vez con más frecuencia.

Francisco Rueda

¿Y los jueces también están preparados en ese mismo sentido para asumir el proceso?

Fredy Bautista G.

Hay avances. Existen algunos que tienen carencias, pero vamos progresando.

María Conchita Jaimes

Tengo una pregunta para Fredy. Si hay una fuga de información porque obviamente la ley es muy clara en judicializar, si soy empleado del Estado hay dos

posiciones. Una que me digan en esa condición usted es responsable de esa información y si hay fuga será judicializado. Si hubo fuga sin intencionalidad de ese empleado, ¿qué sucede?

Fredy Bautista G.

Vienen los niveles de responsabilidad. Hay tres elementos que se tienen que dar en la conducta: la tipicidad, la antijuricidad y la culpabilidad. Lo que ese empleado del Estado hizo puede atacar y ser antijurídico porque afecta la norma como tal y esa conducta está tipificada. Y, además de eso lo contempla la ley, es decir, está tipificada, pero no fue culpable. En esa medida, no se dan los tres elementos mencionados y el resultado final del ejercicio no va a producir señalamientos o imputaciones de cargos, por lo menos a nivel de la categoría de dolo. Y en ese sentido, tenemos muchos casos como ejemplo. Por eso decía que puede quedar en una imprudencia, en una ignorancia, en una negligencia.

Sara Gallardo M.

Por eso este es el país en donde todo pasa y nada pasa.

Fredy Bautista G.

Claro, eso es así.

Se advirtió que la imputación de cargos por fuga de información tiene sus vacíos.

Sergio Pérez B.

Saliéndonos del tema judicial ya en un proceso disciplinario, el funcionario público puede incurrir por omisión o por acción.

Fredy Bautista G.

Pero una de las situaciones que se incorpora dentro del nuevo ordenamiento procesal penal colombiano es la restauración de los derechos de la víctima. Puede que penalmente no responda, pero civilmente sí. No va para la cárcel, pero el bolsillo de ese empleado se verá afectado.

Jeimy J. Cano

Desde el punto de vista corporativo los impactos jurídicos a la fecha no son tan amplios o tan contundentes como se quisiera. Primero, porque la organización no tiene clasificada la información y por otro lado, no ha delegado formalmente la responsabilidad del manejo de la información. Entonces ahí, encontramos una carencia y al crearse un proceso disciplinario interno por temas de fuga, el problema será identificar la prueba. Luego, la respuesta que dará un empleado, frente a esta situación será: "¿en qué parte se me delega formalmente que tengo que manejar la información en esta compañía?". Partiendo de este hecho, las personas se preguntan sobre cómo va a desarrollarse el proceso en su contra.

Juan Pablo Páez S.

Hay rubros asociados a la pérdida de información y simplemente están contemplados.

Jeimy J. Cano

Esa pérdida está relacionada con el P y G, y habrá que cuantificarla. El tema es que la información no tiene la relevancia ni el carácter de activo fundamental ni estratégico para una compañía. Entonces, en tal sentido, mientras esta declaración no se dé, mientras la clasificación de la información no exista y, mientras no sea asignada formalmente la responsabilidad sobre el manejo de la información, internamente dentro de las organizaciones, no habrá casos con la suficiente importancia en torno a la fuga de información.

Francisco Rueda

¿No será que en la empresa existen otras prioridades? Quizás hay otros bienes más importantes de proteger

Fredy Bautista G.

Cuando hacen pública una mala política de la organización en ese sentido, entonces ahí sí lo sienten.

Jeimy J. Cano

Entonces volvemos a lo mismo, el tema de seguridad infortunadamente es reactivo. En este sentido, permítanme hacer una analogía. ¿Qué es lo más importante en un vehículo? ¿Las luces, las marcas, el conductor, el motor...? Y la pregunta siguiente es: ¿usted se subiría en un automóvil a toda velocidad que no tenga frenos? Si su respuesta es no, eso quiere decir, que no podemos ir más rápido, sin unos buenos frenos. Luego, los buenos frenos empiezan por cultura, por tecnología, por asignar recursos, por entender que la información se convierte en la médula espinal de la organización.

Fredy Bautista G.

Encontramos gobiernos corporativos que le temen a la violación de la privacidad de sus empleados, versus la fuga de información. Y en ocasiones gana el empleado y la organización se cuestiona cómo traspasar esa barrera y el asunto se queda en esa dimensión.

Juan Pablo Páez S.

Yo lo asumo como hacer una campaña de mercadeo sin tener el producto. No hay nada listo, pero falta lo principal. Eso quiere decir que hay una carencia de conocimiento sobre la compañía. ¿Qué es lo que duele? En un área financiera, para citar un ejemplo, una información que llegue a ser de conocimiento de la competencia, acaba la compañía. Porque la competencia sabe los movimientos y las estrategias. En una institución de educación hay un grupo de seguridad, la dirección de tecnología y nos dicen la directriz de la entidad es la libre promoción y desarrollo de las personas y si se coarta eso se está violando un derecho fundamental que defiende la universidad. Pero al mismo tiempo, hay que garantizar mi disponibilidad, accesibilidad y el rendimiento de toda la infraestructura tecnológica. Entonces si es la misma universidad la que se ataca y restringe su manera de actuar en torno a la seguridad, entonces ¿qué se hace? Eso va en contravía y es una problemática que estamos afrontando hoy en día.

Sergio Pérez B.

En algunas entidades del Estado ese asunto se está blindando con los contratos. Desde un principio el funcionario o al empleado que va a ingresar se le está sometiendo a ciertas condiciones sobre la intimidad y la privacidad. Anteriormente, si la administración llegaba a emprender alguna acción en lo relacionado con revisión de los escritorios y demás, se recurría a la jurisprudencia donde se realizaba una analogía entre el lugar de trabajo y el lugar de residencia o habitación para efectos de intimidad y privacidad. Es decir, sin una autorización legal no es posible acceder a los elementos personales del empleado. Si la organización no toma las precauciones que debe tomar desde el momento en que incorpora al funcionario, después es muy complicado el manejo del tema.

Jeimy J. Cano

Cuando se hace el análisis constitucional del derecho que tiene la persona a manejar su privacidad, encontramos que es el mismo nivel que tiene la organización para proteger sus activos. Entonces, conciliar dos derechos de nivel constitucional equivalentes, genera un enfrentamiento de dos derechos con el mismo rango y conciliar los mismos, no tarea fácil. Tanto la organización como el empleado están en todo su derecho de exigirlo. Entonces la organización debe considerar desde un principio cómo articular la situación. Sobre la fuga de información y los medios de comunicación –internet, televisión, prensa- a propósito de WikiLeaks ¿cree que hay forma de controlarla, de manejarla? ¿Cuál es su opinión frente a la responsabilidad legal que compete a cada una de las personas involucradas? ¿Considera usted que la naturaleza del dato o la categoría del que publica información confidencial, influyen en la calificación de esta responsabilidad? ¿Cuáles son las lecciones aprendidas? ¿Cómo alertar a los Estados sobre el riesgo de que una fuga de información pueda afectar su gobernabilidad?

Los WikiLeaks y la información que circula por las redes sociales fue también objeto de análisis.

Fredy Bautista G.

El riesgo de la divulgación de tanta información hace que se lleven dos juicios: el penal y el de los medios de la opinión pública. Eso lleva a dos velocidades diferentes. La de la opinión pública se condena, se sataniza, se juzga, se condena y a veces no existe la base legal frente al tema de divulgación de esa información. Y esto tiene que ver no sólo con los Estados, sino con las empresas privadas, el tema de la crisis financiera, la crisis inmobiliaria española de hace tres años, ahora el ciberactivismo. Todo eso conlleva a desde la óptica nuestra aún no hay una política determinada, porque si se responden se genera un efecto contrario y si no se responde se puede generar la sensación de que estamos totalmente desprotegidos frente a lo que pueda ocurrir. Es un asunto bien complejo. Sobre el ciberactivismo ocurrido en los últimos meses, muestra que el poder de las redes sociales hace negativo que se haga cualquier manifestación nuestra sobre ese tipo de acciones, en la medida en que puede generar un ataque peor.

Jeimy J. Cano

Debe haber una posición por parte de la Nación. ¿Hay una directriz de ciberseguridad que faculta al Estado a tomar acciones a través de los entes correspondientes? En este tema tenemos mucho que aprender todavía.

Sergio Pérez B.

Como funcionario especializado en el tema de la seguridad se es muy analítico sobre los riesgos. Lo primero cuando suceden eventos como el de WikiLeaks, es preguntar ¿qué pasara hacia adelante?, ¿qué lecciones debemos aprender, por lo menos para implementarlas y que no sucedan en nuestras organizaciones? A nivel del Estado se siguen realizando esfuerzos fuertes en la implementación de herramientas y políticas estatales, así como de intercambio de información y adhesión a convenios internacionales que coadyuven a las investigaciones judiciales, seguridad de información, prevención y específicamente con reglamentaciones en las que está inmersa la fuga de información. De hecho, son pasos que se han dado muy lentamente por diferentes factores, pero que avanzan y están en las agendas de las entidades que tienen que ver con estos procesos. A nivel interinstitucional hemos tenido avances importantes, y se va a llegar a un punto en que se integrará a las organizaciones privadas y la academia.

María Conchita Jaimes

Esa es una forma de expresar precisamente la falta de mecanismos para controlar la fuga de información. Las redes sociales, los WikiLeaks son el reflejo de tales vacíos. El único medio para combatirlo es un gobierno corporativo claro y con foco en incentivar una cultura de protección y manejo adecuado de la información.

Jeimy J. Cano

Los invito a hacer las conclusiones sobre lo aquí tratado.

Fredy Bautista G.

Insisto en que la fuga de información alimenta un modelo de economía criminal. Es necesario distinguir cuándo la fuga de información corresponde a un hecho accidental o no intencional de los que generan la tipificación de una conducta penal.

Y, en ese sentido, asumo que las organizaciones deben estar preparadas como mínimo en tres frentes: el aspecto cultural de sus empleados, el tecnológico y el gobierno corporativo en torno a la fijación de políticas claras. También es clara la responsabilidad penal que existe en el ordenamiento actual, en las normas y hay desconocimiento frente a las responsabilidades que nos asisten y a unas sanciones de tipo complementario, como la inhabilidad en el ejercicio de las funciones; las responsabilidades de carácter civil frente al tema de la fuga de información.

Serio Pérez B.

Las organizaciones deben continuar con la implementación y madurez en los procesos de gestión de seguridad de la información. Estos son temas complejos y largos que obedecen a procedimientos y cumplimiento de normas establecidos, en los que se deben integrar diferentes estándares y estrategias de seguridad, que definitivamente hay que monitorear y manejar para minimizar los riesgos de cada organización.

María Conchita Jaimes

Definitivamente todavía no contamos con mecanismos para detectar la fuga de información. No hay nada formal, no hay cómo evitarla. Todavía estamos en un nivel de inmadurez y se maneja de manera reactiva.

Juan Pablo Páez S.

Hay que revisar la estructura de las organizaciones, empezando por la motivación a nivel directivo que promueva la creación de políticas y estrategias encaminadas a la implantación de mecanismos que permitan prevenir, además de adoptar una acción reactiva y proactiva. Sistemas que se deben gestionar para que constantemente sean revisados y mejorados para que las organizaciones puedan tratar los incidentes de seguridad. Hoy se habla de DLP, mañana no sabemos cuál será la problemática, pero teniendo una estructura clara dentro de la organización será posible tratarlo. Gobierno y flexibilidad, además de la concientización de la gente sobre el rol fundamental de la información dentro de la organización.

Notas al pie de Página

[1] Tomado de: http://www.lawyerpress.com/news/2009_07/03072009_001.html (Consultado: 12-06-2011)

Sara Gallardo M. *Periodista comunicadora, universidad Jorge Tadeo Lozano. Ha sido directora de las revistas "Uno y Cero", "Gestión Gerencial" y "Acuc Noticias". Editora de Aló Computadores del diario El Tiempo. Redactora en las revistas Cambio 16, Cambio y Clase Empresarial. Corresponsal de la revista Infochannel de México y de los diarios "La Prensa" de Panamá, "La Prensa Gráfica" de El Salvador, y la revista "IN" de la aerolínea Lanchile. Coautora del libro "Lo que cuesta el abuso del poder". Investigadora en publicaciones culturales. Exministra de La Palabra (Gerente de Comunicaciones y Servicio al Comensal) en Andrés Carne de Res. Editora de esta revista desde 1998. Asesora en comunicaciones.*

Diseño de software seguro

Manuel Dávila Sguerra

El software es un elemento catalogado de seguridad nacional en los países que tienen un plan de desarrollo orientado hacia la sociedad del conocimiento. La preocupación en esos países se basa en el hecho de que la Ingeniería de software no ha logrado que los desarrollos de software cumplan con la característica denominada "trusworthy", es decir, digno de confianza. Este artículo pretende recoger una serie de especificaciones que contribuyan a que se cumpla el desarrollo de software seguro. No es la seguridad perimetral la que preocupa en esta investigación, es el software en sí.

Para ello se ha consultado la estrategia de desarrollo de software de los Estados unidos para el 2015, se resumen los planteamientos de Gary McGraw, uno de los líderes en la propuesta de metodologías de software seguro, y se hace una propuesta para incluir en el ciclo de desarrollo las etapas necesarias para lograr estos desarrollos.

Finalmente, haciendo uso de los referentes de ACM e IEEE sobre los diseños curriculares para crear programas de Ingeniería de sistemas o afines, se proponen algunos puntos importantes para incluir en los nuevos programas la formación en este tipo de competencias.

Palabras clave: Software seguro, trustworthy, diseño curricular, Ingeniería de sistemas.

1. Introducción

En los países orientados a conformar sociedad del conocimiento y que tienen en el desarrollo de software un compromiso como industria, se le considera a éste un producto de seguridad nacional. Es el caso de los Estados Unidos que en el reporte de la segunda cumbre del Centro Nacional de Software así lo presenta, en un documento llamado "Software 2015: A national software strategy to ensure U.S. Security and competitiveness" [1]

Consideran que su nación es altamente dependiente de las tecnologías de la información siendo el punto central el software, el cual se encuentra en todos los elementos de la vida cotidiana de las personas y las organizaciones. Determinan que su país es una nación bajo riesgo de consecuencias inaceptables por las fallas del software. Estas fallas pueden crear serios problemas en varios riesgos, enumerando específicamente la infraestructura nacional, la economía, la vida de las personas, la pérdida de confianza pública, de la identidad y liderazgo.

Si bien nuestros países no se comparan con la capacidad productiva de software

que tiene Estados Unidos, es de mucha utilidad conocer esos planes, pues de todas maneras las tecnologías informáticas tienen carácter global. Siendo innegable la importancia del software, así como su penetración en la vida cotidiana se ve la necesidad de revisar el estado de la Ingeniería de software, la cual en sus 50 años de existencia aún no ha podido resolver el riesgo de que un avión se caiga por culpa de un *overflow* en una variable.

Vale la pena anotar que el nivel de seguridad que se necesita en el diseño de los programas va más allá de la tradicional seguridad perimetral, para entrar en el campo del diseño de las aplicaciones.

Este estudio ha contemplado las premisas de la estrategia de los Estados Unidos como referencia para entrar en una discusión de índole más local.

2. Software digno de confianza o trustworthiness

Se introduce el término *trusworthiness* o la cultura sobre las características que debe cumplir el software para ser "trustworthy" o sea, digno de confianza. Estas características se resumen en: seguridad, confianza, fiabilidad y supervivencia. El significado de cada una de estas características se detalla a continuación.

Seguridad: se refiere a la exposición de los programas a peligros no intencionados en sus especificaciones; es decir, que no se dan por mala Ingeniería de software o malas prácticas en la programación, sino por aspectos de índole externo. Cabe hablar aquí de código malicioso y malintencionado como son los virus, troyanos, puertas traseras, spam lo que no sólo crea problemas reales de disminución de confianza, sino que bajan la productividad porque el tiempo de control y revisiones de los daños es muy grande, pudiendo usarse en otras labores más productivas. Una persona que gaste una hora diaria en revisar estos problemas equivale a un mes laboral del año.

Confianza: la vida normal de las personas transcurre con el uso de elementos o artefactos que dependen del software y que su uso debe generar confianza para una tranquilidad de índole social. El software inseguro puede llegar a hacer daño a las personas y a la propiedad en ambientes de uso cotidiano como la aviación, la medicina, la exploración espacial, la banca y en general el transporte. Obsérvese cómo en estas actividades está en peligro la vida de las personas, no sólo una funcionalidad con repercusiones económicas.

Fiabilidad: en algunos casos el software participa de soluciones de gran escala que pueden afectar de manera masiva a la sociedad, como la defensa nacional, las telecomunicaciones, la energía, el espacio y los sistemas financieros. El hecho de utilizar satélites para las telecomunicaciones y el transporte de los datos nos puede afectar.

Supervivencia: ese término se definió como una característica que asegure que el software se debe mantener en continuo funcionamiento, aún en situaciones adversas y no sólo en ambientes benignos. El reciente drama del Japón con el terremoto y el tsunami dan que pensar en cuanto a lo que se puede catalogar una situación adversa, pues los centros de datos deben contemplar estas situaciones y el software mismo también.

Pasemos ahora a determinar una definición formal para la palabra "Trustworthi-

ness". Lo más cercano que he encontrado en español para traducir este término es "Digno de confianza"; es decir, que debe cumplir con todos los requerimientos, inclusive con los de seguridad, en cualquiera de los componentes de software, aplicación, sistema o red.

Un desarrollo de software *digno de confianza,* tiene atributos de "seguridad, garantía, confianza, fiabilidad, rendimiento, supervivencia, con un amplio espectro de adversidades y compromisos. Se requiere en el hardware, en el software, en las comunicaciones, en componentes de potencia, así como en los desarrolladores y los que hacen el mantenimiento". La inclusión del factor humano en estas taxonomías dan que pensar en cuanto a la formación integral de los profesionales en las universidades en donde los aspectos de tipo ético cobran aún más valor.

La estrategia contempla en primer lugar la necesidad de que a la fuerza de trabajo, es decir a los desarrolladores, se les eduque permanentemente y de les defina una estructura salarial adecuada y competitiva.

Le da a la investigación y al desarrollo la verdadera dimensión para fortalecer esta industria invitando a que las Universidades y las empresas trabajen de manera mancomunada, así como el Estado, que debe contribuir desde las instituciones encargadas de diseñar leyes para fomentarlas. Se da una especial atención a los procesos creativos que según García Córdoba en su libro sobre la Investigación aplicada y tecnológica, los define como "la capacidad de generar soluciones finales desde ángulos insospechados" [2]

El estudio determina que no son las buenas intenciones las que lograrán crear software *digno de confianza*, sino una formación profesional y una intención permanente que debe ser involucrada en el ejercicio profesional de los profesionales. Pero no como una opción, sino como una necesidad. Lo anterior requiere entonces de mejores diseños en las métricas de calidad, en el proceso evaluativo, en las metodologías a utilizar en el futuro, en la relación con las empresas y el Estado, desde las universidades.

3. Metodologías de desarrollo tradicionales

La creación de software se orienta por metodologías que se han venido construyendo con el tiempo; y, pensando que esta concesión aporta académicamente al artículo y a la contextualización del problema central, mencionaremos algo al respecto. Sin importar cuál metodología se use, el modelo que presentaremos al final para el desarrollo del software seguro debe ser tenido en cuenta.

Las metodologías más conocidas son:

Modelo Construir y mejorar (1950 – 1960):

Utilizado por la Volskwagen en la producción y venta de sus vehículos cuyo esquema promueve que el artefacto terminado se use, y se recopilen las fallas detectadas por los usuarios para mejorarlo. Hoy en día, a pesar de su popularidad, recibe justificadas críticas .

Método en cascada (1970):

Esta fue la época en que Edsger Dijkstra creó la programación estructurada y funciona si cada fase está perfectamente desarrollada, lo cual casi nunca se cumple. Propone un desarrollo secuencial.

Modelo prototipo rápido:

Se basa en el modelo de las plantas piloto de los Ingenieros Químicos y va produciendo el programa con las funciones esenciales para ir mejorándolo, en la medida en que el usuario los acepta. Es de anotar la presencia del usuario un poco más involucrado en el proceso.

Modelo incremental:

Es una mezcla del modelo en cascada y del prototipo rápido y ya reconoce que los pasos en el desarrollo no son discretos, y va creando construcciones paulatinas, con el peligro de que el proceso de aprendizaje exceda al de la productividad y se de el "síndrome de la investigación".

Modelo Extreme Programming:

Se basa en el desarrollo del sistema de nómina de Chrysler y se involucra al usuario o cliente cuyo "discurso" es recibido en su lenguaje original y se toma como parte del desarrollo, el cual se hace de manera incremental. La Chrysler dice "se monta al usuario en el desarrollo" como una metáfora relacionada con montarlo en el vehículo, pero que significa tenerlo en cuenta de manera preferencial.

Modelo Round Tripping:

Se soporta en los generadores de código basado en diseño de patrones. Está muy orientado a la Programación orientada a objetos.

Modelo Iterativo RUP:

Se considera uno de los más realistas, pues hace seguimiento entre cada estado y el anterior.

El modelo tradicional, que envuelve a la gran mayoría de las metodologías, contempla los siguientes ciclos: especificaciones o modelo funcional, diseño o arquitectura, programación, pruebas, documentación, entrenamiento y mantenimiento. Se acostumbra a expresar la Complejidad del software como una función del tipo de programa (*N*), el número de entradas (*I*), el número de salidas (*O*), y una potencia *p* de tal manera que:

Complejidad = N*I*(O elevado a la potencia p) [3]

4. Seguridad de las aplicaciones y seguridad perimetral

Hasta el momento la seguridad perimetral ha seguido evolucionando cada vez con mayor fuerza. Las gerencias de infraestructura informática tienen más en cuenta la necesidad de incluir proxys y firewall para filtrar el tráfico, tanto al nivel de las URL como de los puertos y servicios de la red. Estos profesionales tienen conocimientos sobre redes y algunos sobre seguridad, ciframiento, certificados de seguridad, detección de intrusos, virus, gusanos, troyanos y de más software intrusivo que llega a la red.

Sobre esto sólo se puede decir que seguirá evolucionando como lo ha hecho, centrando su atención en la capa baja del modelo OSI. En la capa alta están las aplicaciones, a las cuales llegan los usuarios y a veces los intrusos que han logrado pasar los filtros de la seguridad perimetral.

Dice el libro "Computer Crime" de la editorial O'reilly que, en la gran mayoría de los casos, los intrusos entran no por complejos conocimientos de redes, sino por el simple hecho de haber podido atrapar las claves de seguridad de los usuarios. [4]

Cualquiera que sea el caso, surge la pregunta sobre la forma como se protegerá la aplicación a sí misma, bien sea por adecuados trabajos en la etapa de diseño, por fuertes procedimientos de escritura del código fuente o por adecuados análisis de riesgo en la interacción con la plataforma tecnológica. Lo anterior lleva a concluir que es necesario incluir dentro del ciclo de desarrollo del software, cualquiera que sea la metodología utilizada, tareas relacionadas con la seguridad, no ya perimetral, sino de las aplicaciones mismas.

Un inconveniente es el hecho de que los profesionales de las redes y la seguridad de hoy en día, no son los mismos de la Ingeniería de software. Es claro que el diálogo se llevará a nivel de la capa de desarrollo, lo que necesita profesionales aceptados por quienes hacen las aplicaciones; es decir, analistas, arquitectos, programadores y demás especialistas.

La formación de este tipo de profesional es nueva y puede surgir de una mezcla de las alternativas de formación que plantea la ACM y la IEEE en el computing curricula 2005. Este referente plantea cinco procesos formativos que son: Ingeniería de computadores, Ciencia de computadores, Ingeniería de software, Sistemas de información y Tecnología de la información.

No está dentro de este estudio el análisis de este referente, pero basta con decir que el perfil del profesional que se vislumbra para intervenir en el ciclo de desarrollo de software seguro puede estar en una mezcla bien diseñada curricularmente entre Ingeniería de software y Tecnología de la información.

Los diagramas de Computing Curricula de estas dos orientaciones se muestran a continuación, aclarando que el eje horizontal indica nivel de conocimiento desde lo teórico (izquierda) a lo práctico (derecha), y el eje vertical va desde abajo a arriba indicando áreas de profundización, es decir, desde el chip, la electrónica, la plataforma, el software, los lenguajes, las metodologías, hasta la implementación. Bajo esas consideraciones la ACM y la IEEE consideran cinco énfasis sobre los cuales se pueden formar los profesionales. Sin entrar en grandes detalles y dejando al lector la indagación de la lógica de estas gráficas, cada una de las cuales tiene un currículo sugerido, nos referiremos a: ***CE***: Computer Enginering. Forma profesionales que van a diseñar computadores. ***CS***: Computer Science. ***SE***: Software Engineering. ***IS***: Information System. ***IT***: Information Technology.

El gráfico abajo a la derecha sólo insinúa que una Universidad puede diseñar el perfil de los profesionales dependiendo de sus objetivos, como una mezcla de estos énfasis.

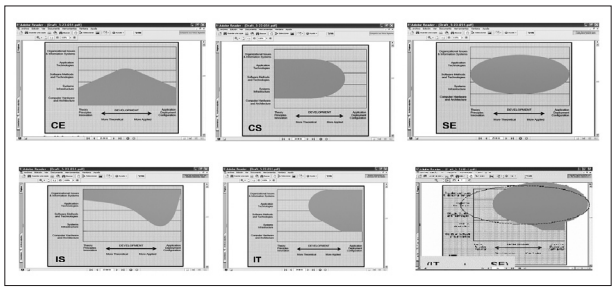


Figura 1. Los énfasis de la Ingeniería de sistemas según ACM e IEEE [6]

En el tema que estamos trabajando, es decir el software seguro, requiere profesionales expertos en SE - Ingeniería de software y con conocimientos sólidos de redes y seguridad IT: Tecnología de la Información.

5. Metodología para diseñar software seguro

Gary McGraw, autor del libro Software Security [5], propone una metodología para incluir dentro del ciclo de desarrollo, la cual puede ser introducida en cualquiera de los modelos de desarrollo que hemos mencionado, pero cabe anotar la importancia de reconsiderar el mecanismo cíclico de cada etapa, para evitar aplicar modelos netamente secuenciales.

En la figura 2 se muestra el ciclo de desarrollo incluido el análisis de la seguridad.

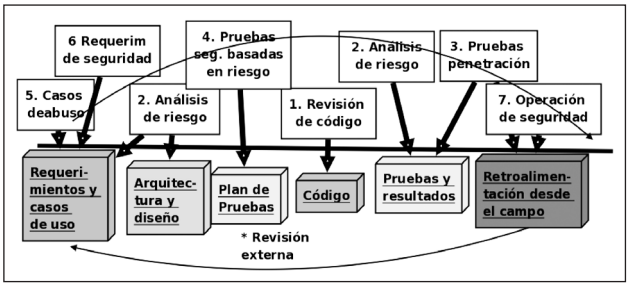


Figura 2. Análisis de la seguridad en el ciclo de desarrollo [7]

Revisión de código con herramientas: el artefacto es el código al cual se le aplica un análisis estático del código fuente, para encontrar riesgos probables. Por ejemplo, buffer overflow encontrado en la línea 8. Este análisis estático busca instrucciones no seguras, pero como todos, no es suficiente por sí solo. ***Análisis de riesgo de la arquitectura:*** el artefacto es el Diseño y especificaciones al cual se le aplica un análisis de los posibles ataques como pueden ser problemas de autenticación o fallas en consideraciones de acceso a la web. ***Pruebas de penetración:*** el artefacto es el ambiente del sistema al cual se debe practicar pruebas de "cajas negras" producidas por otros sistemas, no solamente las pruebas bien conocidas. Un ejemplo puede ser un manejo pobre de la interfaz. ***Pruebas de seguridad basado en riesgos:*** los artefactos son unidades y sistema. Se refiere a los posibles escapes de datos, en donde la mejor actitud es pensar como un atacante. ***Casos de abuso:*** los artefactos son los casos de uso y los requerimientos. Se debe hacer una descripción de las susceptibilidades del sistema bajo ataques bien conocidos. ***Requerimientos de seguridad:*** los artefactos son los requerimientos. Se deben tener en cuenta aspectos como cifrado, certificados de seguridad y en general seguridad funcional. Un riesgo es adolecer de esa descripción. ***Operaciones seguras:*** el artefacto es el sistema en funcionamiento. Se asume que los ataques son inevitables, por lo que se debe tener información para conocer y reconstruir los eventos; por ejemplo, con bitácoras adecuadas.

6. Pérdida de calidad

La calidad de los resultados es el objetivo final del desarrollo de software. Ésta tiene muchas definiciones y mecanismos para lograrla, sin embargo se expondrán los análisis de los autores Bijay K. Jakaswal y Peter C. Patton, autores del libro Design for Trusworthy software [7] basados en las teorías del Dr Genichi Taguchi, japonés nacido en 1924, quien expuso su teoría sobre la pérdida de calidad (QualityLoss), la que define como "La pérdida llevada por el producto a la sociedad desde el momento en que es empaquetado".

El concepto fundamental se basa en la idea de acercarse lo más posible al objetivo propuesto, de tal manera que la variación del resultado final con respecto a él sea la mínima posible y que los niveles de variabilidad conllevan costos de reproceso, mantenimiento, fallas, reclamos, rendimiento y fiabilidad. Se trata de medir este costo como una función cuadrática de la desviación con respecto a la finalidad. Y aplicar una metodología que incremente el control de variables externas a través de lluvia de ideas, investigación y metodologías formales. Insiste, el Doctor Taguchi, en la parametrización que permita ejercer control sobre variables sensibles y ser tolerantes en el sentido de permitir fijar valores a algunos parámetros sobre realidades comprobadas.

Para comprender el tema, el Dr Taguchi incluye una serie de definiciones en su lenguaje que ayudan a comprender sus postulados sobre la calidad como son:

Robustez*:** "un estado en donde el rendimiento de la tecnología, producto o proceso es mínimamente sensitivo a factores que causen variabilidad al menor costo unitario de manufactura". ***Señal: "es lo que un producto debe mostrar por las características de sus funcionalidades". Sonido en un radio, imagen en un televisor, funcionalidades comprobadas en un paquete de software. ***Ruido:*** "factores que causan variaciones externamente, internamente o entre productos". Interferencias en la imagen de un televisor o uso errático por parte del usuario de un paquete de software, ataques, virus, gusanos y huecos de seguridad, poca documentación, entrenamiento inadecuado, malos procedimientos o malos usos del sistema, accesos no autorizados, sometimiento del sistema a usuarios para los cuales no fue diseñado.

Teniendo en cuenta estas definiciones Taguchi resume en algunas premisas el método: "La pérdida de calidad se debe más a fallas después de ventas"; "La robustez de un producto depende más de la etapa de diseño, que del control durante su funcionamiento"; "no liberar nada que no cumpla los estándares"; "no usar medidas de calidad basadas en el usuario"; "los productos robustos producen una 'señal' fuerte sin importar el 'ruido' externo y con un mínimo de 'ruido' interno".

Se sabe que el Señor Deming, llamado el padre del movimiento de la calidad moderna, fue seguido por Taguchi en algunas de sus teorías y propone también una serie de premisas aplicables al desarrollo de software como estas: "atender la voz del usuario o consumidor, reducción de la variación, medidas estadísticas, ganancia de confianza, respeto por los cotrabajadores, mejora continua en el proceso".

Y la esencia de los puntos de Deming que también son aplicables al caso del software son: "constancia en el propósito"; "evitar dependencia de las inspecciones construyendo calidad desde el principio"; "entrenamiento permanente"; " liderazgo más que supervisión ";

"eliminar incentivos por cuotas y cambiarlas por liderazgo"; "eliminar administración por objetivos cuantificados y cambiarlos por liderazgo"; "eliminar los premios por méritos anuales cambiarlo por administración por objetivos"; "educación y auto mejoramiento".

7. Conclusiones

La experiencia vivida en esta investigación he permitido ir creando una metodología formal para que al hacer un proyecto de desarrollo de software sea tenida en cuenta la seguridad en el software. Académicamente, nos permite transmitir a través de conferencias a los estudiantes estas tendencias. Es de esperarse que las asignaturas de Ingeniería de software le den más importancia, en las universidades, a estas innovaciones.

Se corrobora nuevamente que la Ingeniería de software requiere mejoras permanentes y que aún depende demasiado de las destrezas de los diferentes profesionales que actúan en un desarrollo de software. Nos deja las expectativas de ver cómo en los Estados Unidos se resolverá el problema de la Ingeniería de software y nos invita, a profundizar en el desarrollo "digno de confianza".

Dos experiencias se han podido concretar en resultados. Una, la de proponer una metodología basada en lo propuesto por Gary McGraw, otra el desarrollo de un algoritmo que permite detectar intrusos, no en la red sino en la aplicación misma, el cual ha sido implementado en la plataforma *e-Genesis – El generador de sistemas* de mi autoría y con el desarrollo de un método para hacer autodocumentación de software, temas que podrán expandirse en otra publicación.

8. REFERENCIAS

[1] Report of the 2nd National Software Summit, software 2015: A national software strategy to ensure u.s. security and competitiveness Report of the 2nd National Software Summit Center for National Software Studies. Center for National software studies, Reston, 2005, pp.1-32

[2] Córdoba G, La investigación tecnológica, Limusa Noriega Editores, pp 216,, 2005

[3] Patton P, Jayaswal B., Design for trustworthy Software, Prentice Hall, pp 7, 2006

[4] Icove D. VonStorch W., Computer Crime, O'Reilly and Associated Inc, pp51, 1995

[5] G. McGraw, "Software security Building security in", 1er. ed., Addinson Wesley", pp. 3-176, 2006

[6] ACM-IEEE, Computing Curricula, Snapshots: Graphical Views of the Computing Disciplines, ACM-IEEE, pp16,2005

[7] G. McGraw, "Software security Building security in", 1er. ed., Addinson Wesley", pp. 84, 2006

Manuel Dávila Sguerra. *Ingeniero de Sistemas Uniandes, Director Departamento de Informática y Electrónica Uniminuto, Coordinador Académico ACIS, Columnista de Computer World, eltiempo.com: 110 artículos publicados, Autor de e-Genesis- El Generador de sistemas, Mención especial en el Premio Colombiano de Informática 2006, Escogido entre los 25 IT Manager del año 2008 por la revista IT-Manager, Miembro Fundador de ACIS, de Indusoft hoy Fedesoft, de la Red de Decanos y Directores de Ingeniería de sistemas, REDIS, Autor de los libros "GNU/Linux y el software libre" y "Software libre una visión".*

Amenazas persistentes avanzadas, inteligencia y contrainteligencia en un contexto digital

Jeimy J. Cano

Recordar las escenas de agentes encubiertos, revelaciones de información secreta y comandos especializados de asalto, son evocaciones de un pasado, que ahora está presente alrededor del concepto de Amenazas Persistentes Avanzadas. Esta nueva realidad, concentrada en una labor de inteligencia avanzada para recabar información de los empleados de una empresa, establece una renovada estrategia de operaciones especiales, que busca lograr acceso a su infraestructura tecnológica a través del eslabón más débil de la cadena. Por tanto, este documento presenta un análisis sencillo y práctico de esta tendencia, revisando algunas lecciones aprendidas de casos particulares, sugiriendo marcos de acción para enfrentar sus impactos.

Introducción

Dice John Maxwell en su libro "El talento no es suficiente": "La perseverancia no es un asunto de talento. Tampoco de tiempo. Tiene que ver con acabar lo iniciado. El talento provee la esperanza para el logro, pero la perseverancia lo garantiza. (…)". Considerando esta motivadora afirmación, podemos advertir que, aplicada en el *lado oscuro de la fuerza* podemos asistir al escenario de esfuerzos perseverantes de los atacantes para doblegar nuestras defensas y convertirnos en un número más de las numerosas estadísticas de ataques y sistemas comprometidos a nivel global.

Recientemente, venimos observando un renovado interés de los "chicos malos" en el conocimiento de las nuevas tecnologías y tendencias emergentes (computación móvil, computación en la nube y cibercrimen en movimiento) (GROBAUER, B., WALLOSCHEK, T. y STOCKER, E. 2011, GOLDMANN, P. 2011), no para someterlas con la materialización de fallas técnicas, sino como plataformas de enlace para llegar cada vez más a los usuarios y hacerlos parte de sus estrategias de engaño, y así, encontrar nuevas formas de incursionar dentro de los dominios organizacionales y tener acceso a ese activo fundamental para mantenerse competitivo en su sector, como lo es la información.

En este sentido, se abre paso en la literatura técnica de seguridad la sigla APT, en inglés *Advanced Persistent Threat*, cuya traducción en español podría ser *Amenazas Persistentes Avanzadas* -APAv-, la cual no es otra cosa que las nuevas estrategias de los atacantes para tomar por sorpresa a los empleados de las empresas, para comprometer la infraestructura propia de sus organizaciones y tener acceso privilegiado a la información de éstas. Este renovado escenario de ataque, nos muestra que los intrusos mantienen un monitoreo vigilante de la inseguridad de la información, reconociendo en las personas el eslabón más débil de la cadena, para superar las barreras tecnológicas que las empresas puedan tener en su perímetro.

Por tanto, en este breve documento presentaremos algunos detalles de esta nueva tendencia de ataque coordinado y avanzado, para comprender la nueva dinámica emergente de amenazas, que aprovechándose de la movilidad de los usuarios y su marcada necesidad de ubicar sus recursos en la nube, son capaces de estudiar sus comportamientos y perfiles para hacerlos "víctimas útiles", para penetrar las defensas técnicas de las empresas y ganar acceso más allá de lo autorizado.

El ser humano: ¿eslabón más débil o más fuerte de la cadena? Ese es el reto. (CANO, J. 2010)

La información fluye a través de los diferentes medios informáticos que tenemos disponibles. Internet, es la autopista natural donde nos comunicamos y encontramos, para lo cual cada vez que enviamos un mensaje de texto, remitimos un correo electrónico o diligenciamos un formulario en la web, estamos abonando a nuestra sombra digital (LOHR, S. 2008) (lo que dicen los datos disponibles en internet sobre cada uno de nosotros), la cual es y podrá ser interpretada por los intrusos en cualquier momento.

En este contexto, los atacantes constantemente están haciendo reconocimiento de nuestros movimientos, utilizando para ello la información que dejamos en redes sociales, mensajes, registros y publicaciones, los cuales describen nuestros gustos, tendencias y motivaciones, insumos básicos para desarrollar estrategias de ingeniería social, para motivar comportamientos deseados que dejen al descubierto formas de ingresar a infraestructuras tecnológicas o secretos industriales de las empresas.

Teniendo en cuenta lo anterior, con la sobrecarga incremental de información que circula en la red y fuera de ella, establecemos un escenario ideal para ser objeto de engaños y manipulaciones, que vulneren los principios básicos de nuestra privacidad, de la esfera personal, que antes de ser propia de una sociedad dominada por la necesidad de información instantánea, era custodiada y resguarda por la poca movilidad de la misma. Así las cosas, se hace necesario renovar nuestros hábitos y estrategias para proteger nuestra información y aquella que se nos delega para su aseguramiento, sabiendo que los atacantes tienen ahora mayores herramientas y trucos para interrogar nuestros modelos mentales y provocar el tan esperado premio: la fuga de información, que conquiste y alcance su objetivo.

Revisando la etimología de la palabra fuga, encontramos que viene de la palabra *fugare* (en latín espantar, hacer huir), deriva de *fugere* (huir), por esta razón en latín fuga significa las dos cosas: persecución y huída. (Tomado de: http://etimologias.dechile.net/?fugar)

Considerando el origen de la palabra en español y su origen latino, la fuga es un acto en el cual se da una huída y a la vez una persecución. Podría decirse que no existe la huída sin una persecución. Necesariamente el acto de huir, exige una causa que anima a una de las partes a desaparecer del escenario para tratar de evitar ser visto o identificado y hacer más exigente la persecución por la otra parte interesada.

Con los recientes acontecimientos relacionados con la fuga de información (en inglés *information leakage*) se revelan muchos de los secretos mejor guardados de las naciones y la agenda paralela que se mantiene entre los gobiernos para conservar los lazos diplomáticos y acuerdos estratégicos. Si revisamos con cuidado lo que ha ocurrido podemos tener diferentes lecturas y motivaciones para calificar los hechos, bien como la mayor brecha de seguridad que se haya realizado o un acto de real libertad de información.

En cualquiera de los dos casos tenemos una fuga de información, que necesariamente genera una persecución, bien por haber expuesto información clasificada como secreta o altamente secreta, o bien por publicar y mancillar la privacidad natural y propia, tanto de las personas naturales como jurídicas. En este contexto, todos tenemos cosas que sabemos son restringidas y propias de nuestra intimidad, que estamos dispuestos a preservar de la mirada de otros, no porque sean ilegales o prohibidas, sino porque hacen parte de nuestra realidad y personalidad propia. Por tanto, todas las acciones que emprendamos para defendernos ante esta situación estarán justificadas frente a la magnitud de los hechos, sabiendo que las consecuencias de estas acciones tendrán efectos a corto, mediano y largo plazo e impactos en la reputación y buen nombre de los involucrados.

Amenazas persistentes avanzadas -APAv-: una tendencia orientada a los empleados de las empresas

Considerando los impactos que puede tener una fuga de información a nivel corporativo y los constantes intentos de los intrusos por alcanzar las infraestructuras tecnológicas de las empresas, vía la práctica del engaño y manipulación de información disponible en internet, se hace evidente una tendencia o vector de ataque, que busca como objetivo contar con un grado de control de la infraestructura vulnerada, actuando persistentemente para retener el acceso y las posibilidades que éste brinda.

En este sentido, Richard Betjlich, detalla los elementos básicos del adversario que actúa siguiendo los elementos de una APAv, con el fin de comprender mejor su motivaciones y movimientos que nos permitan, más adelante, establecer algunas contramedidas para limitar el accionar de este tipo de amenazas, que buscan comprometer la esencia misma de la ventaja competitiva de las empresas, como lo es su información: (BEJTLICH, R. 2010)

Amenaza significa que el adversario no es una pieza de código sin sentido, al contrario, es una persona motivada, financiada y organizada, que busca un objetivo particular, para lo cual estará bien rodeada y asistida para lograr la misión designada.

Persistente significa que el adversario tiene una tarea que cumplir y que insistirá en ella hasta lograrla. En este sentido, persistente no significa necesariamente que buscará ejecutar un código malicioso en el computador víctima, sino mantener el nivel de interacción necesario para alcanzar sus objetivos.

Avanzada quiere decir que el adversario puede operar un amplio espectro de posibles intrusiones informáticas; es decir, puede utilizar desde las más evidentes y publicitadas vulnerabilidades o elevar el nivel del juego, para investigar o desarrollar nuevas debilidades o fallas, dependiendo de las prácticas de seguridad y control de la empresa objetivo.

Como quiera que este tipo emergente de amenazas no es nuevo, en cuanto se basa en un componente eminentemente humano y asociado con comportamientos de las personas frente al tratamiento de la información, sí representa una importante novedad, cuando se trata de operaciones digitales asistidas con propósitos de espionaje y desinformación, aplicados sobre objetivos gubernamentales, militares o privados.

Casos recientemente publicados y ampliamente difundidos dan cuenta de que este tipo de amenazas han cobrado importantes organizaciones, poniendo en tela de juicio sus posturas frente a la seguridad de la información. A continuación se detallan algunos de ellos, como fuente de documentación y lecciones aprendidas: (SAVAGE, M. 2011)

- El ataque a la firma RSA inició con dos correos phishing con asunto: "2011 Recruitment Plan", enviado a dos pequeños grupos de empleados. Un empleado dio *click* en una de las hojas electrónicas adjuntas en el correo, el cual contenía un *exploit* de día cero, lo cual abrió una brecha de seguridad dentro de la empresa, lo que permitió que los atacantes tuviesen acceso a los sistemas de información críticos de la empresa y paso a la información relacionada con los productos SecureID, del cual son líderes en la industria de seguridad informática.

- Así mismo, tenemos el ataque del grupo "Anonymous" a la firma de seguridad HBGary Federal a comienzos de este año. El ataque consistió en efectuar un engaño a un administrador de red, para que se diese acceso al sitio Rootkit.org, sitio web de investigaciones en seguridad informática mantenido por el fundador de la empresa *Greg Hoglund*, ocasionando desde allí un ingreso no autorizado a la empresa, ganando acceso a los sistemas interno de correo electrónico con datos sensibles y otra información crítica de la misma.

- Finalmente, el ataque a Google efectuado el año anterior, donde los atacantes recolectaron información publicada por los empleados de la firma en redes sociales como *facebook* y *linkedid*. Luego, configuraron un sitio web con fotos falsas, desde donde enviaban correos electrónicos que contenían enlaces al parecer confiables, dado que venían aparentemente de personas de confianza. Una vez, la personas hacía *click* sobre el enlace del correo, se descargaba un código malicioso, que abrió una brecha de seguridad que dio acceso a los servidores corporativos de Google.

APAv, lecciones aprendidas y algunas por aprender

El foco fundamental de una APAv es atacar a los usuarios y no a las máquinas. Es un movimiento psicológico y de comportamiento basado en la información misma de las víctimas, que genera una falsa sensación de seguridad que permite al atacante tener acceso a la infraestructura interna de las organizaciones. En este sentido, es necesario establecer iniciativas de monitoreo de

cruce de información, balancear la necesidad natural de los empleados por descargar información, permitir dispositivos móviles en las redes internas y el acceso a redes sociales; un mundo de intereses cruzados que enfrenta los derechos fundamentales de los individuos y la exposición a los riesgos propia de las empresas con presencia en internet.

¿Qué hemos aprendido de los múltiples casos de uso efectivo de las APAv? Hagamos una mirada crítica sobre tres elementos fundamentales:

1. Nuestra naturaleza orientada a confiar en los demás. Esta condición sana y generosa que dentro de las empresas se genera por un ambiente de camaradería y motivación al trabajo en equipo, se ve mancillada y desvirtuada, frente a las APAv, toda vez que la información expuesta de las personas de la empresa en internet, opera como estrategia de inteligencia para abrazar la confianza de una comunidad, que de manera inadvertida acepta y entiende, que de personas conocidas podemos aceptar mensajes o comunicaciones, generando graves brechas de seguridad que comprometen el buen nombre y los activos intangibles de la empresa.

2. Manejo de las expectativas de las personas. Esta situación propia de los seres humanos se ve oscurecida, cuando un tercero es capaz de conocer o inferir este tipo de deseos o anhelos, en los cuales encuentra el mejor motivador y motor para capturar la atención de sus víctimas. En este sentido, información sobre ascensos, ingresos, nuevos beneficios o incluso retiros de personas de las empresas, se vuelve sensible y clave a la hora de lanzar estratégicamente engaños electrónicos, relacionados con las esperanzas e intereses de las personas en las organizaciones.

3. El afán de compartir información: si no estás en las redes sociales, no existes. Estamos en un mundo donde la información fluye todo el tiempo. Es nuestro deber, saber qué debe circular y qué no, qué información voy a compartir y cuáles serán sus implicaciones al hacerlo. Debemos tomar mejores decisiones informadas sobre los riesgos derivados de ubicar información en los medios electrónicos, sabiendo que al hacerlo estamos minando nuestro propio derecho a la privacidad y control de la misma. Así, mientras más conscientes seamos de la información que tenemos y compartimos, mejores experiencias tendremos al interactuar en la red.

Todo esto nos lleva indefectiblemente a cuestionarnos sobre el contexto futuro y emergente que nos traen las nuevas tendencias tecnológicas y propuestas de servicios, que no hacen otra cosa que motivarnos a mantener información en otros dominios, compartir información con otras personas y movilizarnos todo el tiempo sin restricciones de cables o lugares. Por tanto, se requiere hacer un pare en el camino y comenzar a desaprender nuestros comportamientos actuales y concretar algunas recomendaciones para disfrutar de manera responsable este nuevo entorno abierto, móvil y dinámico que nos proponen los nuevos desarrollos.

En este contexto, a continuación detallamos algunas lecciones que tenemos por aprender frente a los avances de las APAv, que prometen continuar sorprendiendo ahora en un universo personalizado en la nube y con empoderamiento permanente de los usuarios frente al uso de las tecnologías de información y comunicaciones.

1. *Insistir en el valor de la información como activo crítico empresarial.* ¿Por qué no le duele a las personas la información de la empresa? ¿Por qué sólo hasta cuando algo ocurre nos interesamos en el tratamiento de la información? La respuesta es sencilla, no existe un vínculo formal que permita valorar la información, como las cosas propias que afectan la vida de cada individuo. La información es algo externo a su realidad, que sólo es considerada importante, cuando la misma te afecta como persona en cualquier contexto de la vida.

2. *Clasificar la información como práctica natural del tratamiento de la información*. Todos sabemos que manejamos información privada y pública. Nadie quiere que se conozca parte de su vida y obra, a menos que cada uno lo autorice formalmente. De igual forma debería funcionar con la información empresarial, toda ella representa la vida y obra de la firma, mucha de ella habla de cosas que sólo le pertenece a la empresa, mientras otra está diseñada para ser compartida con el entorno. Así, mientras este ejercicio intuitivo que hacemos de manera personal no sea una práctica natural en el entorno corporativo, continuaremos escuchando historias que nunca se debieron contar.

3. *Promover sistemas de inteligencia y monitoreo preventivo sobre el flujo de información empresarial*. Esta consideración advierte a las organizaciones que deben avanzar en el desarrollo de nuevas capacidades de detección de patrones competitivos y de amenazas informáticas en el contexto de sus relaciones de negocio, para establecer acciones preventivas que permitan anticiparse a futuros ataques o amenazas. Esto significa, que la información no será solamente un activo crítico, sino la fuente misma de las acciones de la organización, frente a los retos de seguridad de la información que le sugiera su entorno, teniendo la capacidad de cambiarlo si es necesario.

Reflexiones finales

Cuando hablamos de Amenazas Persistentes Avanzadas –APAv-, no estamos caminando por terrenos tecnológicos o de propuestas de investigación y desarrollo novedosas; estamos recorriendo los senderos de la mente humana, sus motivaciones y sus condiciones en un escenario corporativo. De hecho, estamos caminando por los pasillos de importantes empresas comerciales, con intereses económicos fundados en información crítica como pueden ser patentes, estrategias empresariales o eventos internos que pueden desequilibrar el buen momento de una compañía.

En este escenario, estamos recreando condiciones históricas de espionaje y filtración de información del pasado, donde agentes encubiertos podían establecer importantes contactos y crear redes de manejo de datos, que permitían generar posiciones privilegiadas a empresas o naciones, las cuales eran transportadas o manejadas en sistemas rudimentarios de almacenamiento como microfilms, discos magnéticos o en sencillas cintas magnetofónicas. Así las cosas, ahora en un mundo interconectado, no es necesario estar en los sitios físicos para lograr el objetivo, basta una operación digital planeada para revelar aquello que se había cuidado y poner en aprietos a las empresas más grandes, a través de los más pequeños en la cadena: sus empleados. (BEJTLICH, R. 2010)

Conocer y advertir este tipo de estrategias de inteligencia informática, exige de cada una de las organizaciones, afianzar sus esfuerzos de entrenamiento y prácticas asociadas con el tratamiento de la información, porque cada vez más habrá "comandos especializados" que adelanten operaciones focalizadas para tener información sensible que requiere un tercero, utilizando como puente a alguno de los empleados. Por tanto, mientras más conciencia se tenga del nivel de exposición frente al manejo de la información, mejor será el "mínimo de paranoia administrable" que cada una de las personas debe tener.

En consecuencia y sabiendo que la situación no habrá de mejorar en el corto plazo, desarrolle una función de contrainteligencia informática sustentada en la formación y desarrollo de "firewalls" humanos, que compartiendo información y advirtiendo situaciones fuera de lo establecido, pueda distinguir la asimetría de la inseguridad de la información, a través de patrones de comportamiento emergentes y divergentes.

Finalmente y sabiendo que el adversario será persistente en su misión para lograr el acceso no autorizado, debemos advertirle, que aunque no conocemos qué nuevo movimiento estará planeando, sí estaremos vigilantes y perseverantes para hacerles la vida más difícil, aprendiendo de nuestra maestra la inseguridad de la información.

Referencias

[1] BEJTLICH, R. (2010) Understanding the advanced persistent threat. Information Security Magazine. July. Disponible en: http://searchsecurity.techtarget.com/magazineContent/Understanding-the-advanced-persistent-threat (Consultado: 6-06-2011)

[2] SAVAGE, M. (2011) Gaining awareness to prevent social engineering techniques attacks. Information Security Magazine. May. Disponible en: http://searchsecurity.techtarget.com/magazineContent/Gaining-awareness-to-prevent-social-engineering-techniques-attacks (Consultado: 6-06-2011)

[3] GOLDMANN, P. (2011) Cyber fraud: Why are we still being victimized. Report. White-Collar 101 LLC.

[4] GROBAUER, B., WALLOSCHEK, T. y STOCKER, E. (2011) Understanding cloud computing vulnerabilities. IEEE Security & Privacy. March/april.

[5] CANO, J. (2010) Fuga de la información: Revelando la inseguridad de la información en el factor humano. Diciembre. Publicación en blog. Disponible en: http://insecurityit.blogspot.com/2010/12/fuga-de-la-informacion-revelando-la.html (Consultado: 6-06-2011)

[6] LOHR, S. (2008) Measuring the size of your digital shadow. New York Times. Disponible en: http://bits.blogs.nytimes.com/2008/03/11/measuring-the-size-of-your-digital-shadow/ (Consultado: 6-06-2011)

Jeimy J. Cano, Ph.D, CFE. *Ingeniero y Magíster en Ingeniería de Sistemas y Computación de la Universidad de los Andes. Ph.D en Administración de Negocios de Newport University, CA. USA. Executive Certificate in Leadership and Management del MIT Sloan School of Management. Profesor Distinguido y miembro del Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática de la Facultad de Derecho de la Universidad de los Andes. Examinador Certificado de Fraude – CFE por la ACFE y Cobit Foundation Certificate por ISACA.*

Ciberseguridad y ciberterrorismo

Diego J. Amórtegui T.

Las tecnologías de comunicación, especialmente internet, han abierto un gran universo de posibilidades de acceso a la información, y al mismo tiempo han generado nuevos riesgos que hace unos años no vislumbrábamos. Este es un momento crítico de cambio, hay una gran apertura en las comunicaciones y posibilidades para compartir información en internet, que demanda más seguridad para cada acción que tomemos; es necesario emplear y desarrollar mecanismos de seguridad informática más robustos y amigables, así como generar patrones de conducta que permitan salvaguardar la vida virtual de las personas.

Así mismo, esta gran apertura genera nuevas posibilidades para que los riesgos de la vida real se filtren a la vida virtual de las empresas y las personas. En este caso es el terrorismo y todas las acciones que pueden vincularse a dicha actividad, toda vez que en el caso específico de un ciberataque, las capacidades están disponibles en manos de algunos, como es el caso de las botnets, los cuales pueden ser rentados por unos miles de dólares. Aunado a esto está el anonimato y la posibilidad de estar a miles de kilómetros de distancia para realizar actividades relacionadas al terrorismo.

Universos antagónicos, ciberseguridad y ciberterrorismo

Desde el año 2000 internet era una idea que comenzaba a gestarse en las empresas y hogares colombianos, las velocidades de aquella época eran un logro admirable, en comparación con lo que recibimos actualmente. Hace 10 anos tener una conexión de 256 Kb era un hecho memorable.

A medida que nos hemos ido introduciendo en este mundo virtual de internet, el cual ya tiene permeado hasta los más pequeños rincones de nuestro entendimiento, las formas en las cuales nos comunicamos y exponemos son cada vez más diversas y desconocidas, como por ejemplo twitter, que en 140 caracteres genera un flujo de conversación tan constante que podría rivalizar con cualquier aplicación de chat existente.

De la investigación realizada para identificar las piezas claves de la ciberseguridad encontré que la mayoría de los autores tienen un mismo enfoque, el de la defensa proactiva. En una conferencia de Chema Alonso publicada en *youtube*, de la cual se pueden extractar tips muy valiosos como por ejemplo, la necesidad de contar con los parches del sistema operativo al día, tener un antivirus actualizado, disponer de firewall, passwords robustos, entre otras precauciones. Son elementos esenciales, tips que pueden resultar suficientes para algunos usuarios. En la misma conferencia se advierte sobre el cuidado que se debe tener en los sitios por donde navegamos y la necesidad de disponer de todo el software actualizado, ataques de día 0, hasta pensar en realizar un hardening a nuestro PC. Para algunos esto puede resultar exagerado y para otros sólo sentido común.

Pero, ¿por qué tomar tantas medidas? Manifestar “yo no soy una persona importante”, “a mí que me van a robar si sólo tengo poco dinero en mi cuenta” son comentarios que me hacia una persona con la que hablaba hace poco, y en cierta manera tenía razón, ¿Por qué? Después de analizar sus planteamientos entendí que la respuesta es muy simple: porque hay personas que pueden vivir con un nivel bajo de “ciberseguridad”, porque este es el adecuado para realizar lo que necesitan. Aclaro que, en mi concepto, es bajo el nivel de ciberseguridad de esta persona.

Pero ese antivirus, firewall y la cantidad de “Anti” que nos venden ahora las grandes empresas, ¿van a permitirnos tener un adecuado nivel de seguridad mientras estemos en línea? En mi opinión la respuesta es NO. Para pensar en forma adecuada con relación a la ciberseguridad, debemos imaginar situaciones de riesgo en las cuales podemos vernos en la vida real y simplemente transferir este conocimiento a la actividad virtual, toda vez que hasta hoy, ni McAfee ni Symantec han inventado un guardaespaldas virtual, que pueda mantenernos seguros y vigilados las 24 horas del día. Lo que pueden hacer es sugerirnos qué puede ser potencialmente seguro y qué no. Lo demás queda a voluntad de ese “tic” generado en el dedo índice cuando se observa un link llamativo y hacemos clic.

La ciberseguridad como la conocemos es un tema de muchas entradas y pocas salidas, nuestra vida social en línea poco a poco está sobrepasando la que posiblemente tenemos en la vida real; estamos conectados 24 horas por medio de un blackberry o un Smartphone a internet y a las redes sociales, y como duramente lo aprendí hace poco, *no hay antivirus para facebook*, (me infecté a causa de ese tic que les comenté). Ya instalé un app de bitdefender, el cual estoy seguro podrá ahorrarme unas neuronas para decir no a hacer clic sobre lo que no debo, y éste me solicitó acceso a casi todo mi perfil. En ese momento sentí que entregaba en comodato mi vida virtual, aunque ya puedo orgullosamente decir que soy usuario de un antivirus en la nube.

¿A qué va todo esto? La verdad todos los días es necesario tomar conciencia sobre la información que tenemos y manejamos en la cotidianidad, aunque parezca trivial y sin importancia, para otros es un foco de dinero y en algunos casos poder. El ejemplo de “no tener dinero en la cuenta”, ese dato puede ser útil para los “muleros” aquellas personas que se encargan de conseguir “mulas”, por medio de correos electrónicos, en los cuales les ofrecen una comisión por la recepción de importantes sumas de dinero en sus cuentas personales, haciéndose pasar por compañías extranjeras o nacionales, o también a través de mi cuenta de correo electrónico, que permite a algunos enviar SPAM o en algunos casos, phishing.

¿Qué es ciberseguridad?

Para responder esta pregunta accedí a Internet y coloqué en google, “cybersecurity”. Lo primero que esperé fue encontrar un artículo de Wikipedia que me diera una definición pero, asombrosamente, no lo encontré. Lo más cercano fue una definición de “cybersecurity standards”, con una lista para aplicar, lo que me permitió entender que la

ciberseguridad no es una fórmula mágica. Se trata de “aplicar las medidas necesarias, para garantizar que la identidad virtual de cada persona, pueda ser salvaguardada en las mejores condiciones, además de permitir el acceso adecuado a medios virtuales, ya sean redes sociales, consulta de información de cualquier tipo por cualquier medio de comunicación, usando Internet por medio de dispositivos creados para tal fin”.

Tal vez no es la mejor definición, pero a mi manera de ver es lo más cercano a lo que en mi concepto debe ser la seguridad en ambientes virtuales. De acuerdo con esta definición, creo que no hay un código de mejores prácticas que pueda recomendarnos el mejor camino a seguir, pero si hay algún elemento indicador de que por esa calle virtual roban, pues pueda usar tal consejo para evitar que me pase algo malo. También creo que los señalamientos de Chema son los mejores puntos de partida para identificar nuestra inseguridad virtual, y poder tomar las medidas adecuadas para asegurar en lo posible nuestra vida por tales espacios. Señalo “en lo posible”, porque las actividades ilegales están a la orden del día.

Los malos al acecho

El malware es más silencioso y efectivo, troyanos como Zeus son los ninjas del nuevo milenio, son “callados”, indetectables y pueden acabar con una persona o una empresa en cuestión de segundos. Se acabaron las épocas doradas de los fabricantes de antivirus cuando dominaban el mercado de la seguridad; ahora el malware dicta el paso e impone las tendencias. La seguridad de las compañías ya se ha movido de los antes indispensables firewalls corporativos, a la seguridad del punto final, donde cada vez se ven elementos de software más modernos, con mayores capacidades y completamente integrados con todas las actividades que realizamos, desde el envío de un correo electrónico, hasta el rechazo o aprobación para copiar un archivo sensible en una USB, por medio de un agente de DLP.

También veo cómo mi buzón se llena de correo basura y algunos mensajes legítimos pueden ser clasificados como spam; las técnicas de evasión de firmas son cada vez mejores y, en algunos casos, también son tema de niños. La industria del malware es muy organizada y efectiva, una o unos pocos crean una pieza de software que por ejemplo explota una vulnerabilidad de día 0, otros se encargan de ponerle un propósito, como robarnos todas nuestras claves, accesos, cookies, hacer de la máquina un zombie, hasta patrón de navegación o todas. Y, finalmente, otros se encargan de aprovecharse de nuestro instinto ya casi natural de hacer clic al correo que viene con el virus o dirige a la persona a una página que puede infectar el PC.

El concepto del hacker (usaré este término para hablar de quien busca causar daño o robar información) que muchos tuvimos en la cabeza hace algunos años gracias a Hollywood, ya es tema del pasado; estas personas no son retraídos sociales ni genios y tampoco adictos a los videojuegos, los hackers de ahora son personas con vidas sociales activas, y no son virtuales, trabajan en empresas, estudian en universidades, asisten a fiestas; el hacker de ahora es una persona tan común como cualquiera.

Causar daño ya no la intención, la razón es que ser muy ruidoso no es rentable ni beneficioso. Existen virus que parchan el equipo para evitar que otro pueda tomar control de la máquina; ahora simplemente se envía un troyano a que realice un man in the browser o cualquier otro proceso, para obtener nuestra información y permitirnos el acceso.

En ningún momento digo que el trabajo de hacking esté desvirtuado, de hecho es una práctica que aún se emplea y que cada vez es más prestigiosa, pero al mismo tiempo que ésta se valida en ambientes más y más diversos. Los verdaderos cerebros de las redes de robo de información emplean a estas y otras personas para que hagan uso de su intelecto y puedan sacar provecho de cualquier situación, desarrollando programas, métodos de evasión, mejorando los actuales programas o simplemente haciendo carding cuando la operación lo permita.

La práctica del crimen es cada vez más rentable. Ya se habla de “crime as a service”, en el cual con unos cuantos miles de dólares es posible rentar una botnet con varios niveles de servicio (bronce, plata y oro), además si lo desea puede entregarse al administrador la información deseada; quien renta obtiene acceso a una consola de C&C, donde puede revisar el progreso e información recopilada por este medio.

Describo estas formas de realizar crímenes informáticos, para poner en perspectiva lo fácil que puede ser para un individuo o un grupo de personas realizar ataques de diversos tipos sobre cualquier infraestructura tecnológica, o de comunicaciones. De la misma manera como indagué sobre el significado de ciberseguridad en Google, hice lo mismo con ciberterrorismo, y aunque esta vez sí encontré una definición, no me pareció adecuada. Revisando otros links encontré un muy buen video en youtube sobre ciberterrorismo, vinculado en la página de dragonjar, en este video según Whitfield Diffie (uno de los creadores del algoritmo Diffie-Hellman) el ciberterrorismo es “motivado políticamente, no quisiera llamarlo un crimen motivado con fines económicos, el terrorismo se caracteriza por atacar a una persona inocente y así asustar a alguien más para conseguir que haga algo”.

De acuerdo con el diccionario de la lengua española, el terrorismo es “la sucesión de actos de violencia ejecutados para infundir terror”; por mi experiencia la definición de ciberterrorismo es poder forzar a uno o un grupo de personas a hacer algo, por medio de métodos coercitivos y usando principalmente la internet para lograr sus objetivos, los cuales pueden tener fines políticos, económicos o de cualquier otra índole; en la definición uso el término ***principalmente*** porque el prefijo “ciber” denota un ámbito electrónico, que no necesariamente incluye la internet. Considero también que un ciberataque en un contexto netamente terrorista, es una forma de confirmar el proceso de ciberterrorismo por medio de hechos concretos.

Ahora y según las facilidades actuales, cualquier persona puede ser un ciberterrorista, sólo se necesita el elemento fundamental que es infundir terror entre las personas, ya sea por medio del uso de correos electrónicos, publicaciones en blogs, redes sociales, usando las páginas en internet de los medios de comunicación de un país, el uso de

videos en youtube, tweets, o de la manera en la cual pueda imaginarse. Para ilustrar un poco más esta idea, existen unos muy buenos ejemplos en la página de la escuela asiática de ciber leyes, (en este sitio colocan una definición muy cercana a la que yo planteo como ciberterrorismo). No soy abogado y tampoco quiero enredarme con conceptos y palabras, pero en esta página hay un ejemplo que creo vale la pena resaltar y es el siguiente:

"Un grupo de personas que matan a un hombre de 50 años de edad hospitalizado al darle un medicamento al cual es muy alérgico. Esto es un crimen.
El hombre de 50 años es la cabeza de una comunidad de minorías religiosas y los asaltantes, que pertenecen a otra comunidad religiosa, lo han matado para crear miedo en la mente de la comunidad minoritaria. Aunque esto sigue siendo un delito, también es un acto de terrorismo.
Si los asesinos habían hackeado en la red del hospital y alterado los medicamentos prescritos, entonces sería un acto de ciberterrorismo".

Actos como los del ejemplo son posibles debido a la disponibilidad de comunicaciones a través del mundo, las cuales permiten que un ciberterrorista ubicado en el otro extremo del globo pueda efectuar un ataque contra una organización, el gobierno de otro país o del propio. En el mundo de hoy y como lo mencioné anteriormente, se puede contratar los servicios de una botnet para efectuar el ataque desde múltiples sitios del mundo, disminuyendo la posibilidad de ser encontrado.

Sumado a esto, está la falta de una identidad virtual clara y definida; internet permite que cualquier persona pueda ocultar o cambiar su identidad a gusto, manteniendo en muchas ocasiones un anonimato al momento de efectuar un ataque, siendo los más elementales los cientos de web proxy que se encuentran actualmente en el ciberespacio.

¿Y qué pasa con los hackers?, ahí están, y son una parte fundamental de un proceso de ciberterrorismo, aún no conozco un grupo proclamado como ciberterrorista integrado por hackers, tampoco conozco grupos ciberterroristas.

Los grupos terroristas han empezado a poner más atención al mundo informático y ya tienen capacidades claras de ejecutar acciones contra diversos objetivos. Según un estudio de la universidad de Dartmouth realizado en 2003, unos de los principales grupos de presión a tener en cuenta son los países islámicos, los cuales han trabajado desde hace varios años en mejorar sus capacidades informáticas. Estos grupos no solamente entrenan hackers, también los reclutan, o contratan para efectuar y apoyar los procesos terroristas de estos grupos. Según otro artículo, China también está mejorando sus habilidades técnicas para efectuar este tipo de ataques, pero en mi opinión, esta afirmación no es objetiva, porque la mayoría de los estudios realizados provienen de Estados Unidos.

En el ciberterrorismo, el ciberterrorista no sólo emplea internet como herramienta de coerción, también es usado como medio de propaganda, reclutamiento, entrenamiento,

recaudo de dinero, comunicación, y escogencia de objetivos. No veremos un Google maps con un marcador que diga “bomba aquí”, pero sí es posible usar esta tecnología para planear rutas de acceso y salida de sitios, y con la ayuda de street view, también pueden conocer visualmente el sitio con todas sus características.

También redes sociales como Facebook permiten realizar un perfil a la o las personas que desean convertir en un objetivo; en estas redes sociales es importante tener una buena configuración de qué se publica y cómo, además de tener la certeza de a qué personas permitirles pertenecer a mi círculo social virtual.

Sin dejar a un lado las capacidades técnicas de una persona, es vital recordar que las herramientas más simples pueden ser usadas para planear y en algunos casos ejecutar terrorismo, pero ¿este proceso de uso de tecnologías de internet, trasladado a la vida real, permite definir a un terrorista como un ciberterrorista? Pregunta que en mi concepto es muy difícil de responder, debido al razonamiento sobre el tema que cada persona aplique.

Realizar ataques, generar comunicados entre otros es sólo una parte de las posibilidades que internet le abrió al terrorismo; sólo hay que pensar que las mismas herramientas que protegen la seguridad y confidencialidad de las empresas y personas, así como las que les permiten trabajar en conjunto y a distancia, también son usadas por grupos terroristas en internet, para transmitir mensajes que solamente ellos puedan descifrar.

Dentro de poco me imagino que la lista de los más buscados por el FBI no estará conformada solamente por nombres y fotos, sino también por avatars y nicks; la CIA interceptando e-meetings de webex, células terroristas en second life ubicando objetivos, ciberterroristas usando augmented reality de playstation para planear ataques sin dejar rastros físicos, o reclutamiento y entrenamiento virtual por medio del sistema kinect de la Xbox. De hecho ya hay una ciber carrera armamentista la cual tiene dos frentes, el primero es quién puede tener el troyano más sigiloso y segundo, quién tiene la botnet más grande, y ninguna de estas es liderada por un Estado.

Los gobiernos de algunos países se están armando para protegerse de un ciberataque terrorista, pero aún a muchos (gobiernos y personas) les cuesta quitarse la imagen del fatídico botón rojo con el que podían lanzar un misil y borrar todo al alcance de éste; quizá si pintamos todas las teclas enter del mundo de color rojo, esto pueda generar una conciencia más profunda, porque aún tememos más a una muerte rápida que a una donde nos afecte de a poquitos.

Conclusiones

El momento por el cual estamos viviendo es de cambio y de adaptación, las capacidades que internet brinda en la actualidad son casi ilimitadas, y aún se están descubriendo nuevas posibilidades, tanto para el bien como para el mal. Estar protegido y seguro en la red es una labor de todos los días, y no todos requieren el

mismo nivel de seguridad, el cual puede ser definido de acuerdo con la persona y al nivel de confidencialidad que requiera o desee.

Pero al mismo tiempo que nos adaptamos, el cibercrimen crece y también se adapta a pasos agigantados, generando nuevas preocupaciones que las empresas de seguridad luchan por cubrir, las cuales están disponibles para cualquier persona que desee hacer el mal, incluido los ciberterroristas, quienes están aprovechando en la actualidad estas nuevas posibilidades que ha acarreado la globalización de las comunicaciones, así como los mecanismos de seguridad creados para mantener la seguridad de las personas en el mundo virtual, siempre apoyado con el velo del anonimato que admite internet

Referencias

[1] http://www.youtube.com/watch?v=Y98OyB6bulg
[2] https://www.facebook.com/bitdefender.safego
[3] http://es.wikipedia.org/wiki/Comodato
[4] http://en.wikipedia.org/wiki/Cyber_security_standards
[5] http://blog.fortinet.com/adaptive-crime-services/
[6] http://en.wikipedia.org/wiki/Botnet
[7] http://www.dragonjar.org/ciberterrorismo.xhtml
[8] http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=terrorismo
[9] http://www.asianlaws.org/
[10] http://www.asianlaws.org/library/cyber-laws/defining_cyber_terrorism.htm
[11] http://www.ists.dartmouth.edu/library/164.pdf

Diego J. Amórtegui T. *Ingeniero de sistemas graduado de la Universidad Católica de Colombia ha realizado estudios en redes de datos y seguridad de la información, con nueve años de experiencia laboral en áreas tecnológicas, especialmente en administración de redes y seguridad de la información. Actualmente, se desempeña como Director de seguridad lógica de una importante entidad financiera y cursa estudios de MBA.*

Seguridad Informática en Argentina – Informe 2011

María Patricia Prandini, MAS, Especialista en Seguridad Informática (UBA), CISA, CRISC
Marcia Maggiore, Especialista en Seguridad Informática (UBA), CISA, CRISC

Introducción

Se le atribuye a Bill Hewlett (1930-2001), cofundador de Hewlett-Packard, la frase "No se puede gestionar lo que no se puede medir"[1]. El campo de la seguridad informática no escapa a esta afirmación. En efecto, un proceso efectivo de toma de decisiones en una materia tan crítica como esta requiere necesariamente mediciones válidas sobre lo que está ocurriendo.

Sin embargo, por diversos motivos entre los que se encuentran el hecho de tratarse de un área en constante evolución, la reticencia de las organizaciones para compartir datos sobre los incidentes que las han afectado y la falta de métricas estandarizadas, resulta hoy dificultoso contar con información precisa y actualizada en este campo.

Con esta certeza, por segundo año consecutivo el Capítulo Argentino de ISACA (Information System Audit and Control Association–www.adacsi.org.ar) y la Asociación Argentina de Usuarios de la Informática y las Comunicaciones (USUARIA–www.usuaria.org.ar) se sumaron durante el año 2011 a los esfuerzos de la Asociación Colombiana de Ingenieros de Sistemas (ACIS–www.acis.org.co) y de otras organizaciones de Latinoamérica para colectar información relativa a diversos aspectos de la seguridad de la información en la Región.

La información correspondiente a Argentina fue recopilada tomando como base 61 respuestas válidas, superándose en un 50% la cantidad recibida el año anterior. Si bien esta muestra sigue siendo relativamente pequeña se considera valiosa, toda vez que fue enfocada exclusivamente a personal especializado, directamente ligado a la temática a analizar. Por otra parte, siendo este el segundo año en que se realiza, permitirá fijar tendencias en su comparación con el anterior. Asimismo, debe considerarse que no existe en la región otra iniciativa similar de esta naturaleza y extensión. En tal sentido, queremos agradecer a quienes nuevamente completaron la encuesta y a los que se sumaron este año, con la certeza de que los datos provistos contribuirán a profundizar el conocimiento de la seguridad de la información en la región y en nuestro país.

El presente informe resume mediante gráficos los aspectos más relevantes de la encuesta realizada, la cual estuvo conformada por 31 preguntas de tipo "multiple choice" y formula una serie de conclusiones respecto al estado de la seguridad en nuestro país, en función de las respuestas recibidas.

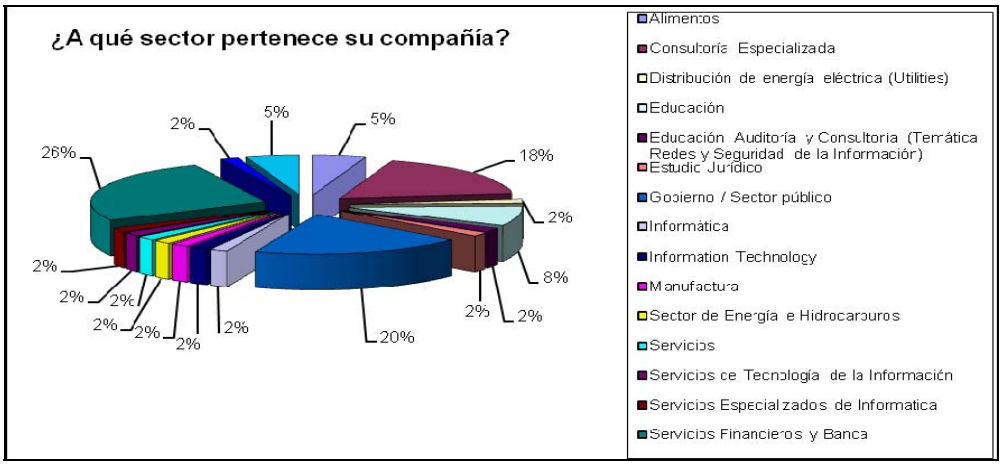
Análisis de datos

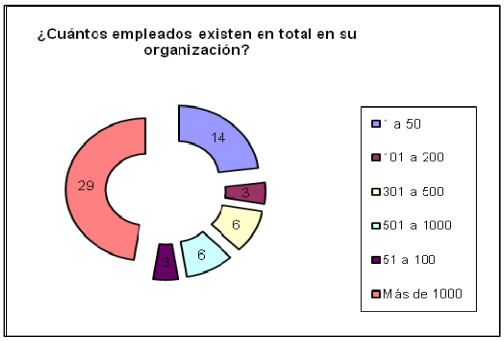
A continuación se presentan los resultados más relevantes de la encuesta mediante gráficos comentados. En los casos aplicables, los datos recopilados se vinculan con los registrados el año pasado.

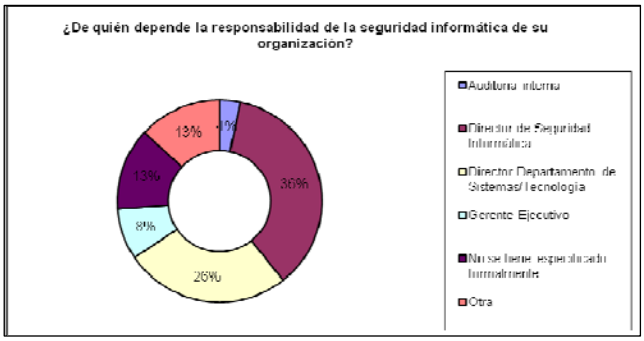
[1] Traducción libre de la frase original en inglés "You cannot manage what you cannot measure"

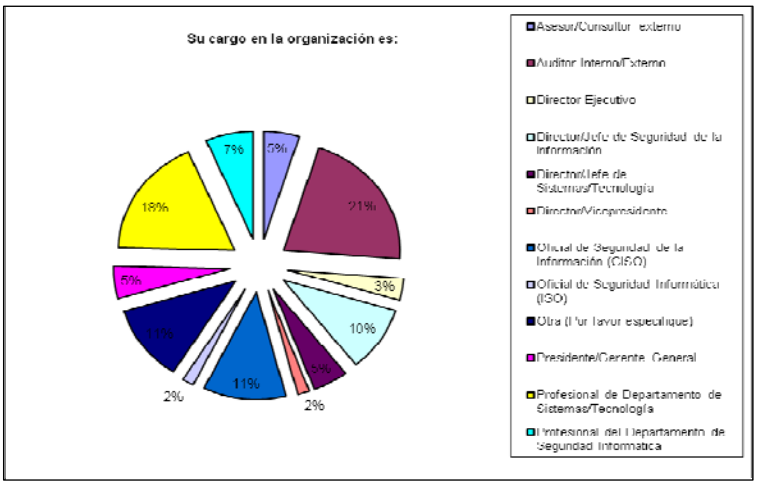
1. Perfil de los encuestados

Esta sección de la encuesta incluye cuatro preguntas vinculadas al sector en que se desempeña el encuestado, la cantidad de empleados que tiene su organización, el cargo que ocupa y el área sobre la que descansan las responsabilidades vinculadas a la Seguridad de la Información.









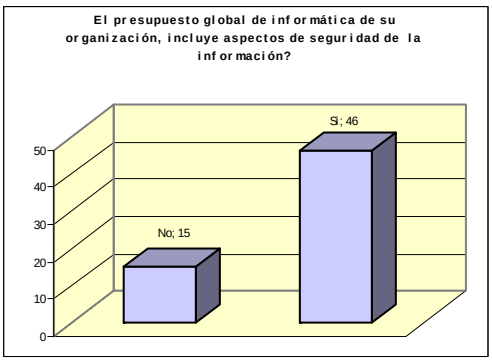
<u>Comentarios generales:</u>

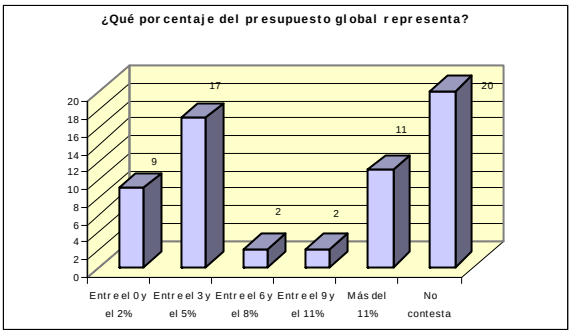
Se observa que la mayoría de las respuestas provienen de profesionales que trabajan en empresas grandes, con plantas de personal que superan el millar de empleados. Si bien este año presenta una distribución levemente más equilibrada, esta característica coincide con los resultados de la encuesta 2010. De los sectores representados, un 25% pertenece

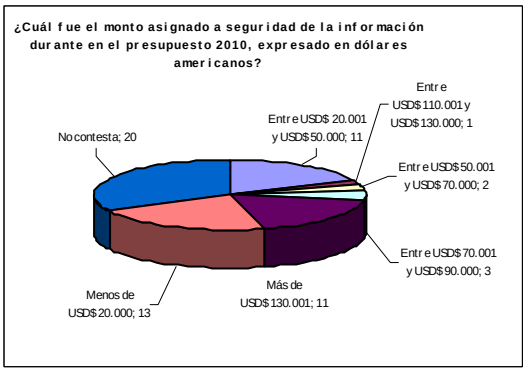
al Sector Financiero seguido del Sector Público y el de Consultoría Especializada. A los sectores ya mencionados, se agregan con porcentajes menores respuestas de los sectores de la Educación, Servicios, Alimentos y Telecomunicaciones, entre otros. En cuanto a los cargos que ocupan los participantes, llama la atención que un 21% son auditores externos/internos, seguidos de personal del área de tecnología y en tercer lugar, del sector de seguridad informática. Un posible motivo para la cantidad de auditores es el hecho de que la distribución de la encuesta se realizó a través del Capítulo local de ISACA, muchos de cuyos socios realizan tareas vinculadas a la auditoría de sistemas. En la encuesta del año pasado, un tercio de quienes respondieron provenía del área de Seguridad Informática, seguidos del grupo de auditores de Tecnología. Respecto a las responsabilidades sobre la seguridad de la información, y mejorando el escenario del año anterior, más de un tercio indica que descansa sobre un área específica mientras que un 26% muestra que depende del área de Tecnología. Sin embargo, el porcentaje de respuestas que señala que las responsabilidades no se encuentran especificadas formalmente es de un 13%, 5 puntos por encima del registrado el año anterior, cuando hubiera sido esperable que la cantidad de respuestas para esta opción hubiera disminuido.

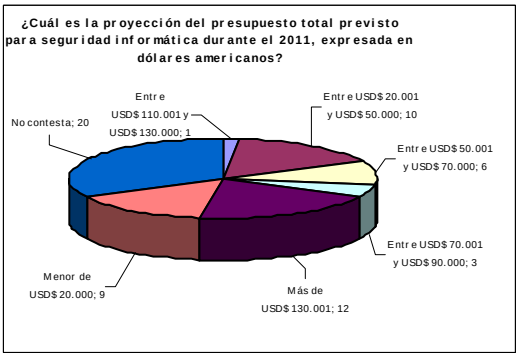
2. Presupuesto asignado a la Seguridad Informática

Esta sección incluye una serie de preguntas relativas a la inclusión en el presupuesto global de la organización de ítems vinculados a la seguridad de la información, al porcentaje que representa, el monto asignado y la proyección para el año 2011.









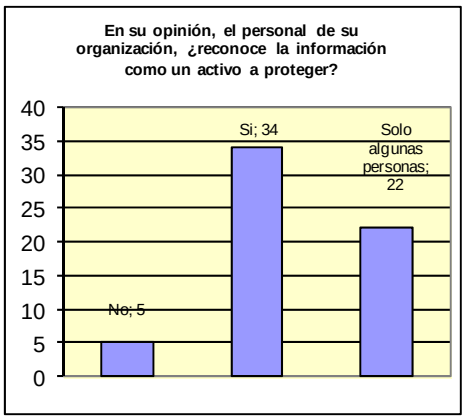
<u>Comentarios generales:</u>

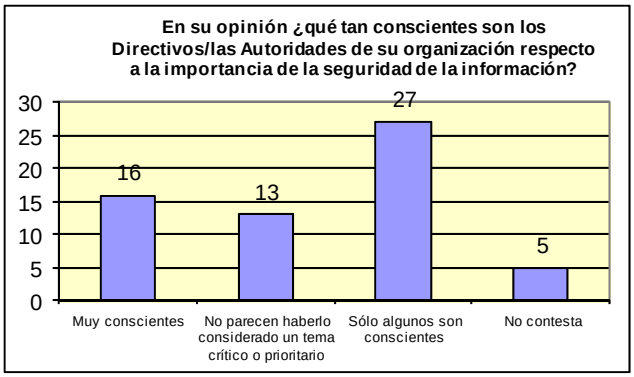
Contrariamente a lo esperado, este año mostró una disminución en el porcentaje de respuestas señalando que el presupuesto asignado al área de Tecnología contaba con partidas específicas para Seguridad. En este caso, sólo un 75% contra el 88% del año pasado, respondió en forma positiva. Sin embargo, al indagar sobre el porcentaje del

presupuesto global asignado al área, un porcentaje mayor se concentró en valores del 3 al 5%, mientras que el año pasado el mayor índice se registró en la opción inferior al 2%. Con relación a la pregunta sobre el monto asignado a la Seguridad, se observa que un tercio no respondió la pregunta, seguramente por desonocer tal asignación. Entre quienes indicaron un monto, nuevamente como el año pasado, las respuestas se mostraron polarizadas. Mientras casi un 20% indicó que contaba con una asignación superior a US$130.000, en el otro extremo, otro tanto señaló contar con menos de US$20.000 dólares. En cuanto a la proyección para el año 2011, y en forma similar a lo ocurrido en la encuesta 2010, se repìtió prácticamente la proporción mostrada en la pregunta anterior. Tal como se señaló el año pasado, estos niveles parecen escasos, a la luz de que, como se vio en secciones anteriores, dentro de los sectores más significativos se encontraban el bancario y el gubernamental, ambos usuarios intensivos de las Tecnologías de la Información, sobre los que basan una parte importante de sus servicios. Por otro lado, resulta desalentador que nuevamente no se prevean mejorías en cuanto a los presupuestos asignados al área de seguridad de la información para el año siguiente, considerando las mayores exigencias regulatorias en la materia y el nivel estratégico de la seguridad de la información para la prestación de los servicios.

3. Nivel de Concientización

En esta sección se presentan las respuestas a dos preguntas vinculadas al reconocimiento del valor de la información como un activo de la organización, desde la perspectiva del personal de la organización y de la de sus directivos y autoridades.



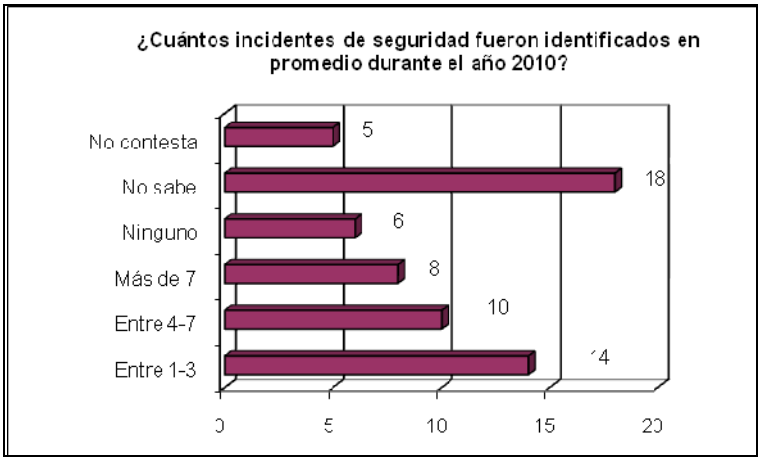


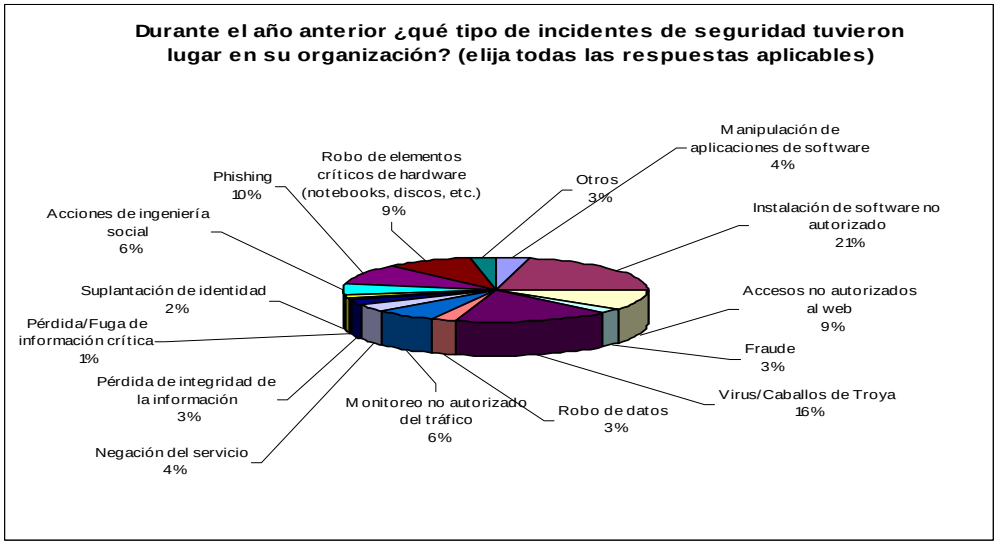
Comentarios generales:

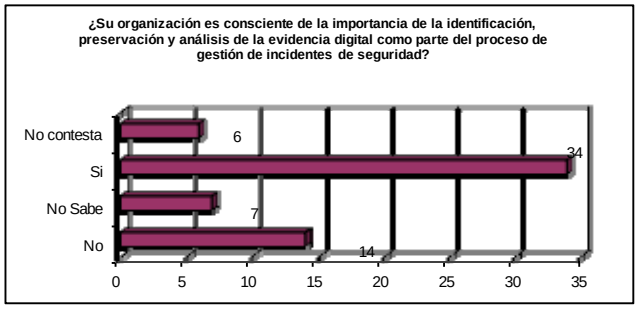
En el caso del primer cuadro, el escenario mejora respecto al año anterior, toda vez que más del 50% indica que el personal es consciente del valor de la información, contra un 21% del año pasado. Sin embargo, esta tendencia se invierte en la segunda opción de respuesta, porque para este año el 33% responde que sólo algunas personas son conscientes, mientras que el año pasado registró un 67%. En cuanto al nivel directivo, un 25% señala que son conscientes y casi un 50% indica que sólo algunos son conscientes. Las respuestas a esta pregunta, que no se formuló en estos términos el año anterior, muestran un escenario desalentador, debido a que un alto porcentaje del personal directivo parece no darle suficiente importancia al tema.

4. Gestión de Incidentes de Seguridad

En esta sección se incluyen preguntas de la encuesta vinculadas a la cantidad y tipo de falla de seguridad y a la evidencia digital.





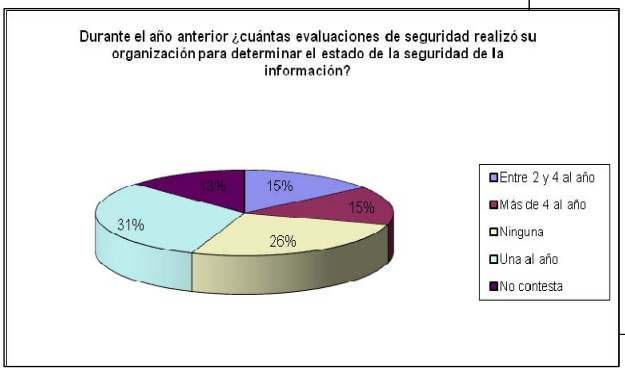


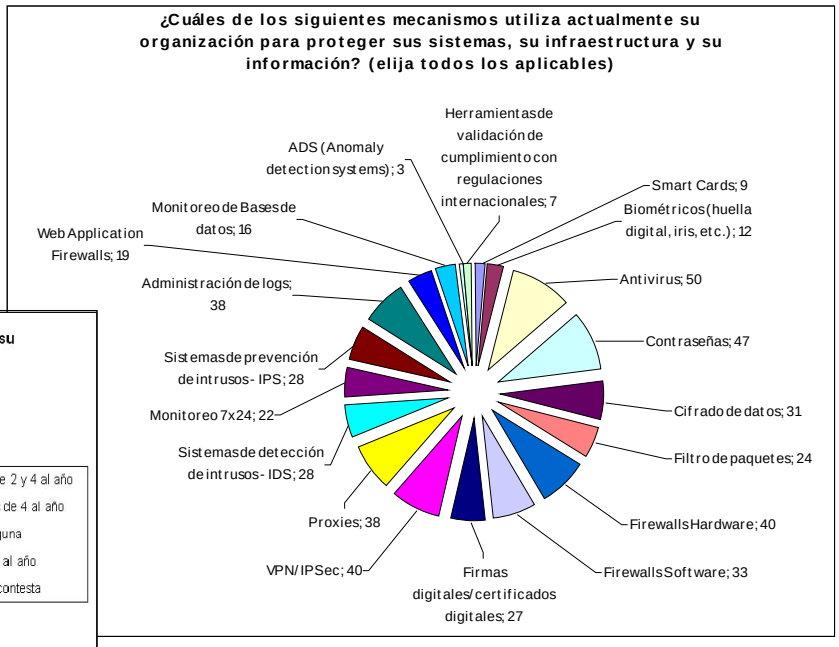
Comentarios generales:

A diferencia de las respuestas recibidas el año pasado, a partir de las cuales podía concluirse que la mitad de los encuestados había tenido entre 1 y 3 intrusiones, este año un 25% señala haber sufrido entre 1 y 3, seguido de un 15% que indica entre 4 y 7 incidentes, mientras que un 30% desconoce la respuesta. Con relación al tipo de incidentes, al igual que el año pasado, los registrados con mayor frecuencia son los virus y la instalación de software no autorizada. Este año le siguen en importancia el phishing, el robo de elementos críticos de hardware y los accesos no autorizados. En cuanto a las preguntas sobre la evidencia digital, al igual que en las encuesta anterior, más de la mitad de los participantes señalan que la organización es consciente de la importancia de la evidencia digital. Sin embargo, sólo un 20% indica que la organización ha aprobado e implementado un procedimiento para su tratamiento. Este porcentaje se encuentra por debajo del registrado el año anterior, que indicaba que un 44% había avanzado en este sentido. Si bien a primera vista, esta observación es desalentadora, debido al tamaño pequeño de la muestra, no pueden tomarse como conclusivas.

5. Evaluaciones de Seguridad

En esta sección se formularon tres preguntas vinculadas a la cantidad de evaluaciones de seguridad realizadas, los mecanismos de protección implementados y la manera en que se tomó conocimiento de las fallas. Se grafica a continuación la primera de las preguntas mencionadas.





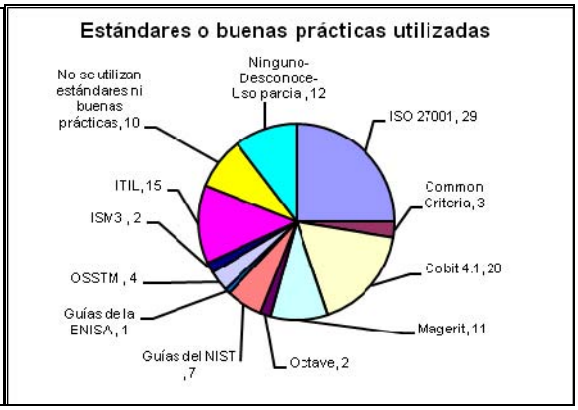
Comentarios Generales

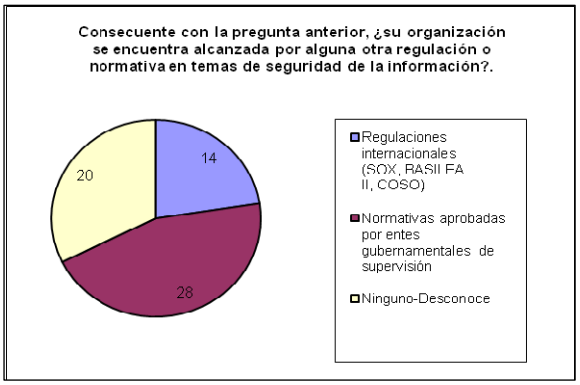
Una de las acciones requeridas por los sistemas de gestión de la seguridad de la información es el monitoreo continuo. Esta actividad resulta importante para corroborar la efectividad de los controles aplicados. En este caso, se observa que la mayoría realiza al menos una evaluación de su seguridad al año, de los cuales un 15% realiza más de 4 y otro tanto, entre 2 y 4. Los valores obtenidos son similares a los del año pasado, habiendo aumentado las respuestas que señalan la realización de más de 4 evaluaciones al año.

Con relación al tipo de mecanismos utilizados para la protección de la información las respuestas también son similares en porcentajes a las registradas el año anterior, siendo las opciones más seleccionadas los antivirus, el uso de contraseñas, las VPN, los proxies y la administración de logs. Cabe acotar que este año se registraron porcentajes algo menores para cada una de ellas. Se aclara que esta pregunta admitía múltiples respuestas.

6. Marco de la seguridad

En esta sección se incluyen preguntas relativas a la existencia de una política de seguridad, los estándares utilizados y las regulaciones que alcanzan a la entidad donde trabaja el participante.



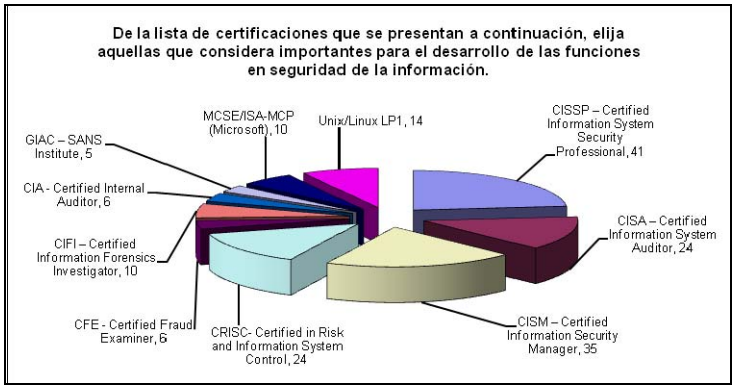


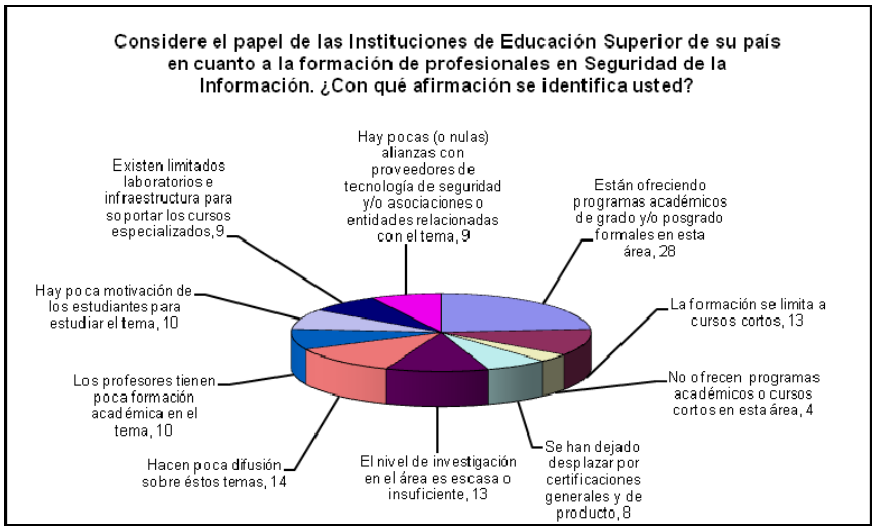
<u>Consideraciones Generales</u>

La definición de políticas es el escalón fundamental para la efectiva implementación de un programa efectivo de seguridad de la información en la organización. Sin embargo, no se observan mejoras en cuanto a la cantidad de respuestas con una política de seguridad escrita, aprobada e informada. Los porcentajes observados son muy similares a los registrados en la encuesta anterior, toda vez que este año algo más de un 50% de las respuestas señalan contar con una política formalizada, un 15% indica que se encuentra en desarrollo y un porcentaje similar responde que la han desarrollado aún. Con relación a los estándares aplicados sigue prevaleciendo la ISO 27001 y el COBIT 4.1 (aunque ambos presentan una proporción menor que el año pasado), seguidos por ITIL y las guías del NIST. Cabe destacar que las normas mencionadas son las más conocidas y respetadas internacionalmente. Respecto a la normativa aplicable, prevalecen aquellas exigidas por los entes gubernamentales de supervisión, seguidas por las regulaciones internacionales, siendo el porcentaje de respuestas recibidas muy similar al registrado en la encuesta anterior.

7. Capital intelectual

En esta sección se engloban las preguntas vinculadas a las certificaciones profesionales y a los programas académicos de formación en seguridad informática.





<u>Comentarios Generales</u>

Aunque con distintos porcentajes y peso relativo es posible observar que las certificaciones destacadas son CISSP, CISA, CISM y CRISC, siendo éstas las más reconocidas en el mercado profesional específico. Cabe destacar con respecto al año pasado, un crecimiento notorio de la Certificación CISM y la aparición de la nueva certificación sobre CRISC, que iguala en valoración a la certificación CISA.

En cuanto a los programas académicos, un 40% indica que se encuentran disponibles mientras que un 25% opina que no se hace suficiente publicidad y que la investigación en la materia es escasa. Respecto al año pasado, ha crecido la percepción respecto a la existencia de programas académicos pero también la opinión respecto a que hay insuficiente investigación.

Conclusión

Si bien -como se dijo más arriba-, este año registró un marcado aumento en las respuestas recibidas, las mismas aún no resultan suficientes como para configurar una muestra representativa. En consecuencia, este informe debe ser interpretado a la luz del

esta circunstancia. Sin embargo, es posible identificar algunos aspectos que, de acuerdo con nuestra experiencia, caracterizan la situación actual en materia de seguridad informática. De igual manera, la existencia de una encuesta anterior permite realizar alguna observación en cuanto a la evolución mostrada. Siguen a continuación algunos comentarios sobre los análisis realizados:

- El porcentaje del presupuesto de TI asignado a Seguridad Informática sigue siendo escaso, teniendo en cuenta la importancia estratégica que la seguridad tiene para una cada vez mayor cantidad de productos y servicios de TI que prestan las organizaciones
- Frente a las preguntas relativas al reconocimiento de la información como un activo a proteger por parte del personal, y al nivel de concientización respecto a la seguridad informática, se aprecian niveles aún bajos, en particular en cuanto a la percepción de los directivos y autoridades. Este es un aspecto crucial para avanzar en una adecuada protección de los datos y de los recursos de información.
- Se reconoce la importancia de la evidencia digital. Sin embargo, es escaso el número de organizaciones que ha establecido procedimientos para su tratamiento. Este tema de creciente importancia al ser cada vez mayor el número de servicios que se prestan por Internet, debe ser atendido en forma urgente a fin de evitar problemas de diversa índole, especialmente legales, en el futuro.
- A diferencia del año pasado que reflejó un reconocimiento del 70%, poco más del 50% de los encuestados afirmó haber sufrido incidentes de seguridad. En cuanto a la tipificación, sigue siendo alto el porcentaje de instalación de software no autorizado, la presencia de virus y el phishing.
- En cuanto a las Políticas de Seguridad, base de cualquier esquema de protección de los recursos de una organización, sigue siendo bajo el porcentaje que manifiesta contar con versiones formales, documentadas e informadas a todo el personal.
- Las certificaciones más apreciadas en las organizaciones continúan siendo CISSP, CISM y CISA, apareciendo este año CRISC, la nueva certificación de ISACA sobre Riesgo, sugida el año pasado. Se destaca también la mayor importancia otorgada a CISM, como certificación de seguridad de la citada organización.

En la medida en que crezca la cantidad de participantes en futuras realizaciones de esta encuesta, será posible contar con una muestra de mayor tamaño que permita avalar en forma más precisa los resultados observados. De esa manera, será posible conocer mejor qué está ocurriendo en nuestro país y en Latinoamérica en materia de seguridad informática, en procura de contar con una herramienta que contribuya a mejorar el proceso de toma de decisiones en esta área de creciente criticidad para las personas, las organizaciones y los países de la región.

Marcia Liliana Maggiore. *Es Computador Científico de la Universidad de Buenos Aires (UBA) y tiene una certificación internacional en Auditoria de Sistemas (CISA), otorgada por ISACA. Ha concluido la Maestría en Seguridad Informática de la UBA, encontrándose actualmente desarrollando la tesis. Es expositora de temas de auditoría de sistemas, control y seguridad de la información para la certificación internacional CIA (IAIA – Instituto de Auditores Internos de Argentina) y las certificaciones internacionales CISA y CISM (ADACSI – Asociación de Auditoría y Control de Sistemas de Información). En su carrera laboral ha desempeñado los cargos de Gerente de*

Seguridad Informática, Coordinador del Comité de Seguridad Informática, Gerente de Auditoría de Sistemas y Coordinador de Auditorías de Procesos en la Administración de Seguridad Social de Argentina, Jefe de la División Auditoría de Sistemas en el Banco Nacional de Desarrollo del mismo país y Jefe de Sistemas en la empresa NOVADATA. Es autora de varios artículos publicados en revistas técnicas y coautora del libro "Normas Internacionales y Nacionales vinculadas a la Seguridad de la Información" junto a María Patricia Prandini. En la actualidad es docente en el Postgrado de Seguridad Informática que se dicta en la UBA.

***Patricia Prandini**. Es Contadora Pública y Especialista en Seguridad Informática de la Universidad de Buenos Aires (UBA) y tiene una Maestría de la Universidad de Illinois, EEUU. Ha terminado de cursar la Maestría en Seguridad Informática en la UBA, encontrándose actualmente desarrollando su tesis. Tiene certificaciones internacionales en Auditoría de sistemas (CISA) y en Riesgo (CRISC) de ISACA. Lideró entre otros proyectos, la implementación de la Infraestructura de Firma Digital de la República Argentina y el ArCERT (Coordinación de Emergencias en Redes Teleinformáticas de la Argentina). Es docente de Auditoría y Seguridad Informática en la UBA, la Universidad Nacional de San Martín y la Universidad Austral. Es presidente del Capítulo Buenos Aries de ISACA y actualmente se desempeña como auditora de Entidades Certificantes en el Estado argentino. Es coautora del libro "Normas Internacionales y Nacionales vinculadas a la Seguridad de la Información" junto a Marcia Maggiore.*

Seguridad de la Información en Latinoamérica
Tendencias 2011[1]

Jeimy J. Cano, Ph.D, CFE
Coordinador Segurinfo

INTRODUCCIÓN

Continuando con el esfuerzo realizado desde 2009, en conjunto con importantes entidades latinoamericanas para conocer los avances y tendencias en seguridad de la información, este año se presentan los resultados de una nueva encuesta para seguir de cerca los movimientos de las prácticas de seguridad en nuestro continente.

En esta ocasión la Asociación Colombiana de Ingenieros de Sistemas (ACIS), el Centro de Atención de Incidentes de Seguridad Informática y Telecomunicaciones –ANTEL- de Uruguay, el Capítulo de ISACA y la organización Usuaria de Buenos Aires, Argentina e ISACA Capítulo Asunción, Paraguay han unido esfuerzos con el fin de revisar el estado actual de la seguridad de la información en nuestra región.

El análisis presentado a continuación se desarrolló basado en una muestra aleatoria de profesionales de tecnologías de información y comunicaciones de Argentina, Colombia, México, Perú, Uruguay y Paraguay, entre otros países, quienes respondieron una encuesta de manera interactiva, a través de una página web dispuesta por la Asociación Colombiana de Ingenieros de Sistemas –ACIS-, para tal fin. Dadas las limitaciones de tiempo y recursos disponibles en la Asociación fueron realizados análisis básicos, los cuales pretenden ofrecer los elementos más sobresalientes de los resultados obtenidos, para orientar al lector sobre las tendencias identificadas en el estudio.

Con esto en mente y considerando otros estudios internacionales como el *13th Annual Global Information Security Survey* realizada por Ernst & Young*,* el *Global State of Information Security Survey 2011,* adelantado por PriceWaterhouseCoopers*;* el *2011 (ISC)2 Global Information Security Workforce Study,* efectuado por Frost & Sullivan; y, el reporte de PriceWaterhouseCoopers *Information Security 2020* se procederá a analizar los resultados de la Encuesta Latinoamericana de Seguridad de la Información 2011.

ESTRUCTURA DE LA ENCUESTA

Fue diseñado un cuestionario compuesto por 35 preguntas sobre los siguientes temas:

- Demografía

[1] Agradecimientos especiales al Ing. Mauricio González, Webmaster y Administrador de la Red de ACIS por su apoyo durante el desarrollo y compilación de los resultados de la Encuesta, así como a la Directora Ejecutiva de ACIS, Beatriz Caicedo, por su apoyo permanente para hacer posible esta iniciativa.

- Presupuestos
- Fallas de seguridad
- Herramientas y prácticas de seguridad
- Políticas de seguridad
- Capital Intelectual

Demografía
Esta sección identifica los siguientes elementos

- Zona geográfica
- Sector de la organización
- Tamaño de la organización
- Responsabilidad y responsables de la seguridad
- Ubicación de la responsabilidad en la organización

Presupuestos
Esta sección muestra si las organizaciones han destinado un rubro para la seguridad de la información de su presupuesto anual. Así mismo, permite revisar el tipo de tecnología en el que invierten y un estimado del monto de la inversión en seguridad de la información.

Fallas de seguridad
Esta sección revisa los tipos de fallas de seguridad más frecuentes; cómo se enteran sobre ellas y a quién se notifican. Por otra parte, identifica las causas por las cuales no se denuncian la fallas y si existe la conciencia sobre la evidencia digital, en la atención de incidentes de seguridad informática.

Herramientas y prácticas de seguridad informática
En este segmento de la encuesta, el objetivo es identificar las prácticas de las empresas sobre la seguridad, los dispositivos o herramientas que con más frecuencia utilizan para el desarrollo de la infraestructura tecnológica y las estrategias que utilizan las organizaciones para conocer sus fallas de seguridad.

Políticas de seguridad
Esta sección busca indagar sobre la formalidad de las políticas de seguridad en la organización; los principales obstáculos para lograr una adecuada seguridad; la buenas prácticas o estándares que utilizan; además de los contactos nacionales e internacionales para seguir posibles intrusos.

Capital intelectual
Finalmente, en esta sección se analiza la situación de desarrollo profesional en torno a conocimientos relacionados con tecnologías de la información: personal dedicado a esta tarea, personal certificado, importancia de las certificaciones y años de experiencia en el tema de seguridad informática

A continuación se presentan los resultados (en porcentajes) de la encuesta por temas y algunos comentarios relacionados con los datos obtenidos:

PARTICIPACIÓN POR PAÍSES

	2009%	2010%	2011%
Argentina	6,50	12,76	**17,13**
Chile	8,80	-	1,97
Colombia	**65,40**	**58,9**	**60,11**
México	12,20	10,3	5,34
Uruguay	7,10	6,07	2,81
Paraguay	-	6,38	0,56
Otros países: Venezuela, Perú, Costa Rica, España, Bolivia, Canadá		5,5	12,08

Comentarios Generales:
En desarrollo de esta tercera encuesta para explorar el estado actual de la seguridad de la información en Latinoamérica participaron 356 (329 participaron en 2010) profesionales en tecnologías de información y carreras afines; Colombia presenta la más alta participación en la misma con un 60,11%, aproximadamente 214 profesionales.

DEMOGRAFÍA

Sectores participantes:

	2009 %	2010 %	2011%
Servicios Financieros y Banca	11,7	**16,71**	**15,56**
Construcción / Ingeniería	4,34	3,64	2,22
Telecomunicaciones	**13,6**	6,07	**13,61**
Sector de Energía	2,4	4	1,67
Salud	3,2	3,34	3,33
Alimentos	1,2	0,91	1,67
Educación	**13,6**	12,76	**16,11**
Gobierno / Sector público	**12,3**	**14,58**	**13,61**
Manufactura	3,8	5,16	1,94
Consultoría Especializada	12,3	**14,58**	13,33
Otros sectores: Asegurador, Logística, Prensa, Fuerzas Armadas, Construcción/Ingeniería, Desarrollo de software	-	18,25	16,95

Comentarios Generales:
A diferencia del año anterior los servicios financieros, Banca, el gobierno/sector público y el sector educativo, junto a otros sectores, fueron los segmentos que

mayoritariamente participaron en la encuesta. Así mismo, muestra una creciente participación de la academia, así como de aquellos sectores en que las regulaciones y exigencias nacionales como internacionales, obligan a las empresas a desarrollar programas alrededor de la protección de la información.

No. De Empleados de la Organización

	2009%	**2010%**	**2011%**
1 a 50	31	20,97	**18**
51 a 100	7,3	**10,94**	**7**
101 a 200	8,5	9,11	9
201 a 300	5,1	**9,72**	5
301 a 500	7,5	8,81	9
501 a 1000	9,1	4,86	12
Más de 1000	**31,4**	**35,56**	**40**

Comentarios Generales:
Los resultados advierten una alta participación de pequeñas y grandes empresas, dos mundos que en su contexto, reconocen la seguridad de la información como elemento diferenciador, generador de confianza y valor para la empresa, sus clientes y grupos de interés. Las empresas en Latinoamérica cada vez más encuentran en la seguridad de la información una forma para marcar la diferencia como socio estratégico del negocio.

Dependencia organizacional del área de seguridad informática

	2009 %	**2010 %**	**2011%**
Auditoría interna	5,1	2,43	5
Director de Seguridad Informática	21,9	26,13	28
Director Departamento de Sistemas/Tecnología	**36,8**	**41,03**	**38**
Gerente Ejecutivo	1,4	2,43	3
Gerente de Finanzas	0,4	-	-
Gerente de Operaciones	2,2	0,3	3
No se tiene especificado formalmente	20,9	13,37	15
Tercerizado	-	-	1
Otros cargos: Superintendente de Comunicaciones y Servicios Técnicos, Gerente de riesgos, Gerente General, Vicepresidencia de Planeación Estratégica del Negocio, Coordinador de Comunicaciones, Líder de Seguridad de la Información		14,31	7

Comentarios Generales:
De acuerdo con la experiencia internacional, el área de seguridad de la información nace de manera natural en el área de tecnologías de información y en

este contexto, Latinoamérica no es la excepción. Este año se confirma la consolidación de áreas de seguridad de la información, con una ligera tendencia de ubicación de éstas fuera del área de tecnología de información. Así las cosas, este resultado nos reta a continuar reescribiendo el concepto de seguridad, desde la perspectiva de negocio para ser parte activa de las estrategias empresariales.

Cargos que respondieron la encuesta

	2009%	**2010%**	**2011%**
Presidente/Gerente General	6,5	4,86	3,06
Director Ejecutivo	3,0	2,43	2,79
Director/Vicepresidente	2,8	1,82	1,67
Director/Jefe de Seguridad Informática	6,9	**15,19**	9,19
Profesional del Departamento de Seguridad Informática	11,9	13,37	**11,70**
Profesional de Departamento de Sistemas/Tecnología	**33,2**	**25,83**	**20,89**
Asesor externo	4,7	5,16	5,01
Auditor Interno	8,7	10,33	**9,75**
Jefe de Seguridad de la Información	-	-	9,19
Jefe de Sistemas y Tecnología	-	-	9,47
CISO – Chief Information Security Officer	-	-	4,46
ISO – Information Security Officer	-	-	3,06
Otros: **Profesores**, operadores, líder de infraestructura, Ingeniero de Proyectos	-	-	**18,94**

Comentarios Generales:
Los resultados en este segmento muestran un importante repunte de la participación de profesionales del área de seguridad informática de las empresas, la confirmación de la colaboración de los profesionales de tecnología de información y los auditores internos, como la población más sobresaliente que dio respuesta a la encuesta. Estos datos nos muestran un avance en la función de seguridad de la información en las organizaciones, que apalancada en ejercicios sistemáticos de auditoría y control, fortalecen los requisitos de cumplimiento y gestión de riesgos, como una forma de generar y comunicar el valor a la gerencia y sus grupos de interés. Se observa una importante participación de profesores este año.

PRESUPUESTO

¿En qué temas se concentra la inversión en seguridad informática?

	2009%	2010%	2011%
Protección de la red	**74,4**	**17,46**	**17,63**

Proteger los datos críticos de la organización	57,9	**14,34**	**13,85**
Proteger la propiedad intelectual	23,1	4,46	4,56
Proteger el almacenamiento de datos de clientes	44,9	10,19	-
Concientización/formación del usuario final	26,7	6,94	6,74
Comercio/negocios electrónicos	16,2	3,37	2,89
Desarrollo y afinamiento de seguridad de las aplicaciones	25,1	5,54	12,54
Seguridad de la Información (normativa y cumplimiento)	53,1	**13,12**	**16,48**
Contratación de personal más calificado	15,1	2,61	4,82
Evaluaciones de seguridad internas y externas	29,2	6,24	7,19
Pólizas contra cibercrimen	6	1,14	0,78
Cursos especializados en seguridad informática (cursos cortos, diplomados, especializaciones, maestrías)	21,3	5,35	5,96
Cursos de formación de usuarios en seguridad informática	12,6	3,12	6,75
Monitoreo de Seguridad Informática 7 x 24	27,7	5,28	6,49

Comentarios Generales:
Latinoamérica sigue una tendencia de la inversión en seguridad concentrada en temas perimetrales, las redes y sus componentes, así como la protección de datos

críticos, reafirmada con un 14,34%. Si estos datos son correctos, aunque la función de seguridad de la información está concentrada en los temas tecnológicos, existe un marcado interés por los temas de cumplimiento normativo y de riesgos, como práctica base en el entendimiento de los procesos de negocio. Estos datos son consistentes con los resultados expuestos en los reportes de PriceWaterhouseCoopers (2011) y Ernst & Young (2011), en los que se ilustran dentro de los *drivers* o movilizadores más importantes del tema de seguridad de la información en las organizaciones, los elementos de cumplimiento normativo, la continuidad del negocio, la reputación de la empresa y las condiciones económicas.

Presupuesto previsto para Seguridad Informática 2011

	2009 %	2010 %
Menos de USD$50.000	**50,3**	**47,72**
Entre USD$50.001 y USD$70.000	17,4	16,41
Entre USD$70.001 y USD$90.000	6,90	10,03
Entre USD$90.001 y USD$110.000	6,20	4,55
Entre USD$110.001 y USD$130.000	4,4	4,55
Más de USD$130.000	14,9	16,71

	2011%
Menos de USD$20.000	**32**
Entre USD$20.001 y USD$50.000	**24**
Entre USD$50.001 y USD$70.000	12
Entre USD$70.001 y USD$90.000	7
Entre USD$90.001 y USD$110.000	4
Entre USD$110.001 y USD$130.000	5
Más de USD$130.000	16

Comentarios Generales:
Aunque las exigencias de nuevos marcos regulatorios y mayores niveles de confiabilidad e integridad, tanto de la información como de los servicios, hacen que el tema de seguridad adquiera la relevancia requerida en las organizaciones, las desaceleraciones económicas mundiales afectan este tipo de inversiones. Los resultados de la encuesta muestran que los presupuestos previstos para la seguridad, se han impactado en las pequeñas y las grandes industrias, sin

perjuicio de que se hayan efectuado provisiones especiales para balancear los efectos de la crisis y mantener los niveles de seguridad actuales, sin comprometer el ambiente de gestión y aseguramiento de la información

FALLAS DE SEGURIDAD

Tipos de fallas de seguridad

	2009 %	**2010 %**	**2011%**
Ninguno	8,1	4,44	-
Manipulación de aplicaciones de software	22,2	4,44	5,48
Instalación de software no autorizado	**60,7**	**18,65**	**17,28**
Accesos no autorizados al web	30,9	9,43	9,87
Fraude	10.8	2,49	4,93
Virus	**70.9**	**20,7**	**16,87**
Robo de datos	9,9	2,06	3,15
Caballos de Troya	**33**	**7,04**	**-**
Monitoreo no autorizado del tráfico	11,4	2,60	3,42
Negación del servicio	15	4,33	5,48
Pérdida de integridad	4,8	1,4	3,01
Pérdida de información	19,5	5,42	-
Suplantación de identidad	13,5	1,84	3,15
Phishing	16,8	4,55	**9,32**
Pharming	3	0,54	1,37
Fuga de Información	21	7,37	3,56
Robo de elementos críticos de hardware	-	-	7,54
Acciones de ingeniería social			4,52
Otras (Espionaje)	-	1,3	0,96

Comentarios Generales:
Los resultados de la encuesta establecen que la instalación de software no autorizado, los virus (incluidos los caballos de Troya) y el phishing son las tendencias más representativas para establecer los retos propios que el área de seguridad de la información considera necesarios para alinear sus esfuerzos, no sólo para instalar tecnologías de protección, sino para comprender las implicaciones de negocio y los atributos de seguridad requeridos en los mismos. Esta tendencia se confirma en el informe de FROST & SULLIVAN 2011, donde se muestra como principales amenazas, las vulnerabilidades en las aplicaciones, los virus y gusanos, así como los dispositivos móviles.

Identificación de las fallas de seguridad informática

	2009%	2010%	2011%

Material o datos alterados	24,6	11,93	13,09
Análisis de registros de auditoría/sistema de archivos/registros Firewall	**47,7**	**23,86**	**26,66**
Sistema de detección de intrusos	**36,0**	**17,95**	**20,95**
Alertado por un cliente/proveedor	23,7	10,12	12,38
Alertado por un colega	19,2	10,84	-
Seminarios o conferencias Nacionales e internacionales	2,7	2,35	2,85
Notificación de un empleado/Colaborador	**37,8**	**23,68**	**24,04**

Comentarios Generales:
Cada vez más los registros de auditoría adquieren importancia en el ejercicio de la función de seguridad de la información. En este contexto, se nota a las organizaciones confirmando que, a través de la atención de incidentes se hace claro y real el nivel de gestión y generación de valor que exige el negocio del área de seguridad. El análisis detallado de registros en los sistemas y una adecuada implementación de sistemas de detección de intrusos, son elementos claves para detallar lo que ha ocurrido.

Notificación de un incidente de seguridad informática

	2009 %	2010 %	2011%
Directivos de la organización	-	-	**44,76**
Asesor legal	19,5	17,23	10,46
Autoridades locales/regionales	10,8	8,30	4,45
Autoridades nacionales(Dijon, Fiscalía)	10,2	5,53	9,13
Equipo de atención de incidentes	35,7	41,23	**18,04**
Ninguno: No se denuncian	**39,3**	**27,69**	**13,14**

Comentarios Generales:
Las cifras muestran un importante aumento de los equipos de atención de incidentes en la región y un marcado reporte de los incidentes a los ejecutivos de las empresas, lo cual sugiere una mayor participación de este nivel en las organizaciones, frente a fallas que se puedan presentar. Sin embargo, continúa una porción importante que no denuncia y envía un mensaje contradictorio y carente de interés, hecho que anima a la delincuencia organizada a continuar avanzando y generando confusión entre los nuevos ciudadanos de la sociedad de la información y el conocimiento.

Si decide no denunciar

	2009%	2010%	2011%
Pérdida de valor de accionistas	9,6	9,17	13,46

Publicación de noticias desfavorables en los medios/pérdida de imagen	28,5	**30,17**	**22,84**
Responsabilidad legal	22,5	18,04	10,54
Motivaciones personales	25,8	21	11,42
Vulnerabilidad ante la competencia	23,4	21,59	**17,71**
Pérdida de clientes actuales/potenciales	-	-	16,39
Posibles pérdidas no significativas	-	-	7,61

Comentarios Generales:
El manejo de la imagen y la vulnerabilidad ante la competencia frente a posibles fallas o pérdidas de seguridad de la información son elementos fundamentales de una empresa, traducidos en bienes intangibles, que apalancan la posición de una organización en un segmento de mercado. En este sentido, la encuesta de PriceWaterHouseCoopers de 2011, muestra que las empresas se deben concentrar en la protección de sus datos, priorización de inversiones de seguridad basadas en riesgo y el fortalecimiento de los programas de gobierno, riesgo y cumplimiento, de tal forma que puedan avanzar en el logro de sus objetivos aún en situaciones desfavorables. Si esto es correcto, los incidentes no deberían impactar la imagen de las empresas; al contrario, deberían fortalecerlas y reconocerlas por su compromiso con el cliente y su propio gobierno.

HERRAMIENTAS Y PRÁCTICAS DE SEGURIDAD

Número de pruebas de seguridad realizadas

	2009%	2010%	2011%
Una al año	**30,3**	**30,3**	**40**
Entre 2 y 4 al año	29,1	26,74	23
Más de 4 al año	14,7	9,11	7
Ninguna	25,9	20,36	30
En blanco	-	13,37	-

Comentarios Generales:
Los resultados de esta sección son contrastantes. Por un lado, un grueso de la población adelanta al menos una prueba al año, mientras el 30 % no hace ningún esfuerzo en ese sentido. Estas cifras deben llevarnos a meditar en la inseguridad de la información, ese dual que constantemente cambia y nos hace pensar sobre las posibilidades a través de las cuales los intrusos pueden materializar sus acciones. Las pruebas no van a agotar la imaginación o posibilidades que tienen los atacantes para vulnerar nuestras infraestructuras, pero sí nos dan un panorama de lo que pueden hacer y nos ayudan a destruir el síndrome de la “falsa sensación de seguridad”. Por tanto, no hacerlo es arriesgarse a ser parte formal de las estadísticas de aquellos para quienes la seguridad es sólo un necesario referente tecnológico.

Mecanismos de Seguridad

	2009 %	2010 %	2011%
Smart Cards	14,4	2,25	1,99
Biométricos (huella digital, iris, etc.)	25,6	2,63	3,64
Antivirus	**86,3**	**11,04**	**11,07**
Contraseñas	**81,9**	**10,92**	**10,57**
Cifrado de datos	48,8	6,45	6.09
Filtro de paquetes	31,6	4,75	4,52
Firewalls Hardware	57,2	**8,32**	**8,47**
Firewalls Software	**62,5**	7,43	7,62
Firmas digitales/certificados digitales	32,5	5,31	4,98
VPN/IPSec	50	**8,03**	7,58
Proxies	49,1	6,50	6,89
Sistemas de detección de intrusos - IDS	36,3	4,08	4,82
Monitoreo 7x24	29,7	3,27	3,79
Sistemas de prevención de intrusos - IPS	25,9	4,16	4,33
Administración de logs	35,6	4,37	5,02
Web Application Firewalls	25,9	3,23	2,68
ADS (Anomaly detection systems)	6,3	0,97	0,68
Herramientas de validación de cumplimiento con regulaciones internacionales	8,8	1,18	1,14
Monitoreo de Bases de datos			4,02
Otros: tokens, cifrado de discos, herramientas de análisis de riesgos, filtro de contenidos	-	0,42	-

Comentarios Generales:
Las cifras en 2011 muestran los antivirus, las contraseñas y los firewalls de hardware como los mecanismos de seguridad más utilizados, seguidos por los sistemas de firewalls de software y las VPN. Dichas tendencias son complementarias con los resultados de la 13th Encuesta de seguridad de Ernest & Young (2011), donde la inversión en seguridad de la información se concentra en la implementación de tecnologías de Data Leakage Prevention –DLP-, planes de continuidad de negocio y tecnologías de gestión de accesos e identidades.

¿Cómo se entera de las fallas de seguridad?

	2009%	2010%	2011%
Notificaciones de proveedores	36,3	21,05	17,38
Notificaciones de colegas	43,1	20,25	18,28
Lectura de artículos en revistas	**58,4**	**28,7**	**23,86**

especializadas			
Lectura y análisis de listas de seguridad (BUGTRAQ, SEGURINFO, NTBUGTRAQ, etc.)	49,1	22,64	20,49
Alerta de CSIRT			12,45
No se tiene este hábito.	16,6	7,33	7,52

Comentarios Generales:
La lectura de artículos en revistas especializadas y la lectura y análisis de las listas de seguridad son las fuentes de información más frecuentes para notificarse sobre fallas de seguridad. Aunque sabemos que la dinámica del día a día limita el tiempo para el estudio permanente de la dinámica de la inseguridad, se consolida la importancia de dedicar un espacio en la agenda de los responsables de la seguridad, para la comprensión y revisión de las fallas de seguridad y su impacto en la organización. SEGURINFO, se ubica como una lista en español referente en los temas de seguridad de la información en Latinoamérica.

POLÍTICAS DE SEGURIDAD

Estado actual de las políticas de seguridad

	2009%	2010%	2011%
No se tienen políticas de seguridad definidas	24,40	14,85	24
Actualmente se encuentran en desarrollo	**41,60**	**43,84**	**33**
Política formal, escrita documentada e informada a todo el personal	34,10	41,30	43

Comentarios Generales:
Los resultados de este año establecen que el 57% de las empresas en Latinoamérica, no cuentan con una política de seguridad definida formalmente o se encuentra en desarrollo. Este resultado no muestra un avance significativo en el reconocimiento de la información, como un activo fundamental de la organización. Considerando que los informes de FROST & SULLIVAN (2011) y ERNST & YOUNG (2011) muestran que las tecnologías móviles, la computación en la nube y las redes sociales son las tendencias que mayor impacto van a tener en el ejercicio de los responsables de la seguridad de la información, las organizaciones no pueden posponer el entendimiento de los riesgos de la información ahora en un contexto abierto, móvil y social.

Principal obstáculo para desarrollar una adecuada seguridad de la información

	2009%	2010%	2011%
Inexistencia de política de seguridad	10,40	13,04	10,78
Falta de tiempo	12,70	13,4	11,71

Falta de formación técnica	10,10	4,71	9,18
Falta de apoyo directivo	**18,50**	15,21	**16,37**
Falta de colaboración entre áreas/departamentos	14,00	10,86	**19,04**
Complejidad tecnológica	7,50	9,78	7,19
Poco entendimiento de la seguridad informática	14	**18,47**	**16,37**
Poco entendimiento de los flujos de la información en la organización	4,20	5,79	9,32
Otras respuestas:	-	8,74	-

Comentarios Generales:
La falta de colaboración entre áreas, el apoyo directivo y el limitado entendimiento de la seguridad son los rubros más sobresalientes en esta sección. Si bien el año anterior, la tendencia marcaba el bajo entendimiento de la seguridad, este año se muestra que la colaboración entre las áreas es clave para comprender mejor los riesgos de los flujos de información en el negocio. Este resultado nos debe alertar sobre el lenguaje que se utiliza para presentar y comunicar el tema, y la necesidad de traducir el mismo en una expresión natural de la dinámica de los negocios.

Contactos para seguir intrusos

Respuesta	2009%	2010%	2011%
No	**52,9**	**50,36**	**50,16**
No Sabe	37,7	35,50	34,44
Si, ¿Cuáles?	9,4	14,13	15,38

Comentarios Generales:
No es de extrañar que exista una relación directa entre la no denuncia de conductas punibles en medios informáticos o a través de tecnologías de información, con el desconocimiento de la existencia de entidades para el reporte de dichos eventos; bien sea por pérdida de reputación o por el riesgo de imagen que implica para la organización. Adicionalmente, dada la limitada aplicación de las normas o regulaciones vigentes en temas de delito informático en Latinoamérica, adelantar un proceso jurídico puede resultar más costoso para la organización que para el posible infractor, toda vez que generalmente la carga de la prueba está a cargo de la parte acusadora y los posibles costos derivados de peritaje informático o análisis forense, no ayudan con la economía procesal.

De acuerdo con lo expresado en el informe de PriceWaterhouseCoopers (2010), el mundo se verá enfrentado en 2020 a una explosión de datos, a una sobrecarga de información. En tal sentido, los gremios, el gobierno, los proveedores y los usuarios deben organizarse para enfrentar al crimen organizado, que busca comprometer la información crítica de los negocios, mediante engaños o ataques, lo que exige de cada uno de los actores, una postura de seguridad resiliente y proactiva que, no es otra cosa que reconocer a las personas como fuente primaria de las fallas y las estrategias de protección.

Estándares y buenas prácticas en seguridad informática y regulaciones en seguridad de la información

Estándares y buenas prácticas	**2009%**	**2010%**	**2011%**
ISO 27001	**45,8**	**26,37**	**28,88**
Common Criteria	5,2	2,10	3,65
Cobit 4.1	23,4	**14,88**	**14,62**
Magerit	5,2	3,23	2,74
Octave	2,3	1,29	2,19
Guías del NIST (National Institute of Standards and Technology) USA	12,3	8,09	7,49
Guías de la ENISA (European Network of Information Security Agency)	2,3	0,97	1,46
Top 20 de fallas de seguridad del SANS	7,1	2,91	-
OSSTM - Open Standard Security Testing Model	7,5	3,23	4,38
ISM3 - Information Security Management Maturiy Model	3,9	0,97	1,46
ITIL	26,9	**17,47**	**18,28**
No se consideran	**37,7**	**10,19**	**14,80**

Norma	**2009%**	**2010%**	**2011%**
Ninguna	**52,30**	**46,95**	**42,94**
Regulaciones internacionales (SOX, BASILEA II)	15,60	13,62	17,05
Normativas aprobadas por entes de supervisión (Superintendencias, Ministerios o Institutos gubernamentales)	33,80	39,42	40

Comentarios Generales:
Los resultados sugieren que en Latinoamérica el ISO 27000, ITIL y el Cobit 4.1 el estándar y las buenas prácticas están en las áreas de seguridad de la información o en los departamentos de tecnología informática. Estas orientaciones metodológicas procuran establecer marcos de planeación y acción en temas de tecnologías de información y seguridad, que permitan a la organización ordenar la práctica de dichas áreas. Este resultado coincide con lo expuesto en el informe de Ernst & Young (2011), donde se identifica que las organizaciones están considerando, entre otros elementos de control, las técnicas de cifrado de datos, el fortalecimiento de la gestión de identidades y accesos y el incremento de las capacidades de auditabilidad de los sistemas.

En ese mismo sentido, las regulaciones sobre seguridad de la información lideradas por regulaciones internacionales como SOX y Basilea II, en contraste con un alto porcentaje que no debe acogerse a ninguna de ellas, muestra que los esfuerzos en seguridad de la información son parciales y sectorizados, lo que implica que se requiere una dinámica similar a la de Banca y el mercado accionario, para generar un esfuerzo común en procura de una cultura de seguridad de la información más homogénea y dinámica.

CAPITAL INTELECTUAL

Número de personas dedicadas a Seguridad Informática

	2009 %	**2010 %**	**2011%**
Ninguna	34,30	18,84	29
1 a 5	**44,10**	**45,59**	**49**
6 a 10	11,80	5,47	9
11 a 15	3,70	3,95	3
Más de 15	6,10	**7,59**	**10**
En blanco	-	18,54	-

Comentarios Generales:
Los resultados muestran que en Latinoamérica existe un número reducido de personas dedicadas de tiempo completo a los temas de seguridad de la información; bien sea por el tamaño de las organizaciones, como por sus prioridades actuales. Así mismo, se nota un ligero aumento de empresas que no tienen destinados profesionales en los temas de seguridad de la información; se sugiere un cambio de prioridades en las inversiones de la empresa, frente a los exigentes movimientos económicos globales.

Años de experiencia requeridos para trabajar en seguridad informática

	2009 %	**2010 %**	**2011%**
Ninguno	21,5	3,34	5
Menos de un año de experiencia	11,8	5,47	3
Uno a dos años	29	28,57	36
Más de dos años de experiencia	**37,7**	**44,07**	**56**
En blanco	**-**	18,54	-

Comentarios Generales:
En la región se confirma una clara tendencia hacia aquellos profesionales que cuentan con más de dos años de experiencia en temas de seguridad informática. Pese a que en la actualidad, los cursos especializados y el entrenamiento autodidacta frente a los dilemas de seguridad es la constante, es interesante observar cómo se exige cada vez más una formación más concreta y formal para

los analistas y consultores en seguridad de la información en la región, esto con relación al 5% donde se no se exige ninguna experiencia en el tema.

Certificaciones en seguridad informática

	2009 %	2010 %	2011%
Ninguna	**57,9**	**37,23**	**34,86**
CISSP - Certified Information System Security Professional	20,5	16,4	**15,23**
CISA - Certified Information System Auditor	13,8	14,3	**14,42**
CRISC – Certified Risk and Information Systems Control			**3,80**
CISM - Certified Information Security Manager	11,8	**13,5**	12,02
CFE - Certified Fraud Examiner	4	2,34	1,80
CIFI - Certified Information Forensics Investigator	4	3,1	2,60
CIA - Certified Internal Auditor	8,4	4,68	5,61
SECURITY+	8,4	4,68	5,61
GIAC-SANS	-	2,86	3,40
NSA IAM/IEM	-	0,78	0,60

Comentarios Generales:
Los resultados muestran que en Latinoamérica el tema de seguridad de la información no requiere formalmente temas de certificación, sino más experiencia aplicada y prácticas de seguridad. Esto significa que aunque se registra limitada oferta de formación académica en el tema, certificaciones como CISSP, CISA y CISM marcan una tendencia y preferencia entre los profesionales latinoamericanos dedicados a los temas de seguridad de la información. Resulta interesante ver el reciente posicionamiento de la nueva certificación de ISACA, denominada CRISC.

Certificaciones en seguridad informática requeridas para ejercer la función de seguridad

	2010	**2011**
CISSP - Certified Information System Security Professional	**23,36%**	**20,77**
CISA - Certified Information System Auditor	**14,67%**	**12,32**
CISM - Certified Information Security Manager	**17,39%**	**16,37**
CRISC - Certified Risk and Information Systems Control		9,82
CFE - Certified Fraud Examiner	4,78 %	4,74
CIFI - Certified Information	**8,04**%	**7,75**

Forensics Investigator		
CIA - Certified Internal Auditor	6,86%	5,34
MCSE/ISA-MCP (Microsoft)	5,65%	4,13
Unix/Linux LP1	5,65%	7,02
GIAC – Sans Institute		**4,05**
Security+	**7,28%**	**5,77**
NSA IAM/IEM	2,06	1,81

Comentarios Generales:
Esta pregunta nos confirma la importancia que tienen en el mercado las certificaciones en el tema de seguridad de la información. Las certificaciones CISSP, CISM y CISA son las más valoradas por el mercado y las que con mayor frecuencia son solicitadas en términos contractuales. Se advierte un particular interés en las certificaciones CIFI y Unix/Linux LP1 que, a pesar de no aparecer referenciadas con altos porcentajes, sí son consideradas importantes por la industria. Las certificaciones son interesantes referentes internacionales, pero se requiere fortalecer la formación académica formal en los temas de seguridad, control y auditoría, así como en las áreas de manejo de fraude, como una estrategia complementaria para el fortalecimiento de la protección de los activos.

Papel de la educación superior en la formación de profesionales de la seguridad de la información

Respuestas	%2010	2011%
Están ofreciendo programas académicos formales en esta área	**22,38**	**14,15**
Existen limitados laboratorios e infraestructura para soportar los cursos especializados	3,73	9,88
Hacen poca difusión sobre éstos temas	5,59	11,23
Hay poca investigación científica en el área	4,85	**12,69**
Hay poca motivación de los estudiantes para estudiar el tema	1,11	5,39
Hay poca oferta (o nula) de programas académicos en esta área	**26,11**	3,70
Hay pocas (o nulas) alianzas con proveedores de tecnología de seguridad y/o agremiaciones relacionadas con el tema	2,61	10,77
La formación es escasa y sólo a nivel de cursos cortos	**15,67**	**12,24**
Los estudiantes no conocen las oportunidades laborales en esta área	2,98	-
Los profesores tienen poca formación académica en el tema	4,10	9,32
No han pensado adelantar programas académicos o cursos cortos en esta área	3,35	-

Se han dejado desplazar por certificaciones generales y de producto	7,46	10,67

Comentarios Generales:
Las respuestas de este numeral contemplado por segundo año consecutivo muestra un ligero aumento de programas académicos formales en seguridad de la información, con un llamado concreto para la academia para que exista una mayor investigación científica en esta área, que permita balancear el uso de las tecnologías disponibles con el desarrollo de propuestas innovadoras, fruto de un entendimiento más profundo de la seguridad en las organizaciones. La invitación es a aunar esfuerzos para consolidar una formación práctica y académica sólida para las nuevas generaciones de analistas y ejecutivos de la seguridad de la información.

CONCLUSIONES GENERALES

Los resultados generales que sugiere la encuesta podríamos resumirlos en algunas breves reflexiones:

1. Los resultados sugieren que en Latinoamérica el ISO 27000, ITIL y el Cobit 4.1 el estándar y las buenas prácticas están en las áreas de seguridad de la información o en los departamentos de tecnología informática.
2. La industria en Latinoamérica exige más de dos años de experiencia en seguridad informática, como requisito para optar por una posición en esta área. Se advierte con énfasis, la necesidad de una formación más concreta y formal para los analistas de seguridad en la región.
3. Las certificaciones CISSP, CISA y CISM continúan como las más valoradas por el mercado y las que a la hora de considerar un proyecto de seguridad de la información marcan la diferencia para su desarrollo y contratación. Resulta interesante ver el reciente posicionamiento de la nueva certificación de ISACA, denominada CRISC.
4. Latinoamérica sigue una tendencia de la inversión en seguridad concentrada en temas perimetrales, las redes y sus componentes, así como la protección de datos críticos. De igual forma, existe un marcado interés por el aseguramiento de los flujos de información en la organización, como práctica base en el entendimiento de los riesgos en los procesos de negocio.
5. Las cifras en 2011 muestran los antivirus, las contraseñas y los firewalls de hardware como los mecanismos de seguridad más utilizados, seguidos por los sistemas de firewalls de software y las VPN. Existe un marcado interés por las herramientas de prevención de fuga de información y tecnologías de gestión de accesos e identidades.
6. La pérdida de reputación, el riesgo de imagen y la vulnerabilidad ante la competencia son factores claves, frente a la denuncia o no de una conducta punible en medios tecnológicos. Adicionalmente, la carga de la prueba frente a los hechos ocurridos está a cargo de la parte afectada y los

posibles costos derivados del peritaje informático o análisis forense se cuestionan frente a la efectividad de los mismos.

7. La lectura de artículos en revistas especializadas y la lectura y análisis de las listas de seguridad son las fuentes de información más frecuentes para notificarse sobre fallas de seguridad. SEGURINFO, se ubica como una lista en español referente en los temas de seguridad de la información en Latinoamérica.
8. La falta de colaboración entre las áreas, el apoyo directivo y el limitado entendimiento de la seguridad, no pueden ser excusas para no avanzar en el desarrollo de un sistema de gestión de seguridad. La inversión en seguridad es costosa, pero la materialización de inseguridad puede serlo mucho más.
9. Los resultados de este año establecen que el 57% de las empresas en Latinoamérica no cuentan con una política de seguridad definida formalmente o apenas se encuentra en desarrollo. Este resultado no muestra un avance significativo en el reconocimiento de la información como un activo fundamental de la organización.
10. Se refleja un ligero aumento de programas académicos formales en seguridad de la información, además de un llamado concreto a la academia para que exista una mayor investigación científica en esta área, que permita balancear el uso de las tecnologías disponibles con el desarrollo de propuestas innovadoras fruto de un entendimiento más profundo de la seguridad en las organizaciones.

REFERENCIAS

[1] ERNEST & YOUNG (2011) *13th Annual Global Information Security Survey.* Disponible en: http://www.ey.com/Publication/vwLUAssets/Global_information_security_survey_2010_advisory/$FILE/GISS%20report_final.pdf (Consultado: 12-06-2011)

[2] PRICEWATERHOUSECOOPERS (2011) *Global State of Information Security Survey 2011.* Disponible en: http://www.pwc.com/gx/en/information-security-survey/pdf/giss-2011-survey-report.pdf (Consultado: 12-06-2010) (Consultado: 06-06-2010)

[3] FROST & SULLIVAN (2011) *2011 (ISC)2 Global Information Security Workforce Study.* Disponible en: https://www.isc2.org/uploadedFiles/Industry_Resources/FS_WP_ISC%20Study_020811_MLW_Web.pdf (Consultado: 12-06-2010)

PRICEWATERHOUSECOOPERS (2010) *Information Security 2020*. Disponible en: http://www.pwc.co.uk/eng/publications/revolution_or_evolution_information_security_2020.html (Consultado: 12-06-2010)

Jeimy J. Cano. *Ph.D, CFE. Ingeniero y Magíster en Ingeniería de Sistemas y Computación de la Universidad de los Andes. Ph.D en Administración de Negocios de Newport University, CA. USA. Executive Certificate in Leadership and Management del MIT Sloan School of Management.*

Profesor Distinguido y miembro del Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática de la Facultad de Derecho de la Universidad de los Andes. Examinador Certificado de Fraude – CFE por la ACFE y Cobit Foundation Certificate por ISACA.