Seguridad de la Información en Latinoamérica
Tendencias 2010[1]

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

INTRODUCCIÓN

Continuando con el esfuerzo realizado en conjunto en 2009, 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; la Red Latinoamericana de Expertos en Derecho Informático (Alfa-Redi de Perú-); la Superintendencia de Servicios de Certificación, Sucerte de la República Bolivariana de Venezuela; la Universidad del Valle de Atemajac, Campus Guadalajara; el Colegio de Profesionistas en Computación del Estado de Hidalgo, México; 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 de Argentina, Perú, Venezuela, Colombia, México, Uruguay y Paraguay, 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, fue realizado un conjunto de análisis básico para ofrecer al lector los elementos más sobresalientes de los resultados obtenidos sobre las tendencias identificadas en el estudio.

Con esto en mente y considerando otros estudios internacionales como el *12th Annual Global Information Security Survey* realizado por Ernst & Young*;* el *Global State of Information Security Survey 2010,* adelantado por PricewaterhouseCoopers*;* el *2010 TMT Global Security Study* efectuado por Deloitte & Touche; y, el reporte de Forrester *The state of Enterprise IT Security and emerging trends: 2009 to 2010,* se procederá a analizar los resultados de la Encuesta Latinoamericana de Seguridad de la Información 2010.

Estructura de la encuesta

[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.

Fue diseñado un cuestionario compuesto por 34 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 sección muestra si las organizaciones han destinado un rubro para la seguridad de la información dentro 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, identifican las causas por las cuales no se denuncian la fallas y si existe 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; 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, por parte del personal dedicado a esta tarea; de quienes están certificados y la importancia de las certificaciones; además de los que cuentan con años de experiencia en el rubro de la 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%**
Argentina	6,50%	12,76%
Chile	8,80%	-
Colombia	**65,40%**	**58,9%**
México	12,20%	10,3%
Uruguay	7,10%	6,07
Paraguay	-	6,38%
Otros países: Venezuela, Perú, Costa Rica, España, Bolivia		5,5%

Comentarios generales:

En desarrollo de esta segunda encuesta para explorar el estado actual de la seguridad de la información en Latinoamérica, participaron 329 profesionales en tecnologías de información y carreras afines, frente a 434 de 2009. Colombia registra la más alta participación, con un 58,9%, aproximadamente 194 personas.

DEMOGRAFÍA

Sectores participantes:

	2009 %	**2010 %**
Servicios Financieros y Banca	11,7	**16,71**
Construcción / Ingeniería	4,34	3,64
Telecomunicaciones	**13,6**	6,07
Sector de Energía	2,4	4
Salud	3,2	3,34
Alimentos	1,2	0,91
Educación	**13,6**	12,76

Gobierno / Sector público	**12,3**	**14,58**
Manufactura	3,8	5,16
Consultoría especializada	12,3	**14,58**
Otros sectores: Asegurador, Logística, Importador, Farmacéutico, Retail, Desarrollo de software	-	18,25

Comentarios generales:

A diferencia del año anterior, los servicios financieros y Banca, el Gobierno/sector público y la consultoría especializada, junto con otros sectores, fueron los segmentos con mayor participación en la encuesta. Así mismo, muestra con claridad aquellos sectores donde las regulaciones y exigencias, nacionales e internacionales, obligan a las empresas a desarrollar programas alrededor de la protección de la información.

No. de Empleados de la organización

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

Comentarios generales:

Los resultados advierten una alta participación de pequeñas y grandes empresas, dos mundos que en su contexto, reconocen a la seguridad de la información como un elemento diferenciador, generador de confianza y valor para la empresa, sus clientes y grupos de interés. Las empresas en Latinoamérica siguen avanzando en la adopción y puesta en práctica de estrategias de protección de la información, que les permite competir en escenario global.

Dependencia organizacional del área de seguridad informática

	2009 %	**2010 %**
Auditoría interna	5,1	2,43
Director de Seguridad Informática	21,9	26,13
Director Departamento de Sistemas/Tecnología	**36,8**	**41,03**
Gerente Ejecutivo	1,4	2,43
Gerente de Finanzas	0,4	-
Gerente de Operaciones	2,2	0,3

No se tiene especificado formalmente	20,9	13,37
Otros cargos: Administrador de sistemas, Outsourcing, Gerente de riesgos, Gerente General, Gerente Administrativo		14,31

Comentarios generales:

De acuerdo con la experiencia internacional, el área de seguridad de la información nace de manera natural en el espacio de tecnologías de información; y, en este contexto, Latinoamérica no es la excepción. Este año se confirma un crecimiento importante de la función de seguridad de la información, centrada en las áreas de tecnología, con una ligera disminución en el rubro de "No se tiene especificado formalmente". 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%
Presidente/Gerente General	6,5	4,86
Director Ejecutivo	3,0	2,43
Director/Vicepresidente	2,8	1,82
Director/Jefe de Seguridad Informática	6,9	**15,19**
Profesional del Departamento de Seguridad Informática	11,9	13,37
Profesional de Departamento de Sistemas/Tecnología	**33,2**	**25,83**
Asesor externo	4,7	5,16
Auditor Interno	8,7	10,33

Comentarios generales:

Los resultados en este segmento muestran un importante repunte de la participación de ejecutivos del área de seguridad informática de las empresas y la confirmación de la colaboración de los profesionales de tecnología de información, como la población más sobresaliente que dio respuesta a la encuesta. Estos datos nos indican que se avanza en un nivel de madurez de la función de seguridad de la información en las organizaciones, que aunque camina de manera decidida para ser un aliado tecnológico del negocio, todavía requiere comprender mejor cómo generar y comunicar el valor a la gerencia y sus grupos de interés.

PRESUPUESTO

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

	2009%	2010%
Protección de la red	**74,4**	**17,46**
Proteger los datos críticos de la organización	57,9	**14,34**
Proteger la propiedad intelectual	23,1	4,46
Proteger el almacenamiento de datos de clientes	44,9	10,19
Concientización/formación del usuario final	26,7	6,94
Comercio/negocios electrónicos	16,2	3,37
Desarrollo y afinamiento de seguridad de las aplicaciones	25,1	5,54
Seguridad de la Información	53,1	**13,12**
Contratación de personal más calificado	15,1	2,61
Evaluaciones de seguridad internas y externas	29,2	6,24
Pólizas contra cibercrimen	6	1,14
Cursos especializados en seguridad informática(cursos cortos, diplomados, especializaciones, maestrías)	21,3	5,35
Cursos de formación de usuarios en seguridad informática	12,6	3,12

Monitoreo de Seguridad Informática 7 x 24	27,7	5,28

Comentarios generales:

Latinoamérica sigue una tendencia de la inversión en seguridad concentrada en temas perimetrales, redes y sus componentes, así como en la protección de datos críticos, panorama reafirmado con un 14,34%. Si estos datos son correctos, la función de seguridad de la información, aunque está concentrada en los temas tecnológicos, 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 proceso de negocio. Estos datos, son consistentes con los resultados expuestos en el reporte de Forrester (2010), en el que la función de seguridad continúa concentrada en los elementos tecnológicos, generalmente animada por cumplimiento de regulaciones y normas internacionales.

Presupuesto previsto para seguridad informática 2010

	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

Comentarios generales:

Si bien 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. En los resultados se observa que los presupuestos previstos para la seguridad se han impactado, tanto en las pequeñas como grandes industrias, sin perjuicio de que provisiones especiales se hayan efectuado para balancear los efectos de la crisis, y así 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 %**
Ninguno	8,1	4,44
Manipulación de aplicaciones de software	22,2	4,44
Instalación de software no autorizado	**60,7**	**18,65**
Accesos no autorizados al web	30,9	9,43
Fraude	10.8	2,49
Virus	**70.9**	**20,7**
Robo de datos	9,9	2,06
Caballos de troya	**33**	**7,04**
Monitoreo no autorizado del tráfico	11,4	2,60
Negación del servicio	15	4,33
Pérdida de integridad	4,8	1,4
Pérdida de información	19,5	5,42
Suplantación de identidad	13,5	1,84
Phishing	16,8	4,55
Pharming	3	0,54
Fuga de Información	21	7,37
Otras	-	1,3

Comentarios generales:

Mientras el informe de Deloitte and Touche de 2010 muestra claramente que los hallazgos más frecuentes identificados por la auditoría, en el ejercicio de seguimiento y verificación son: exceso de privilegios, falta de registros de auditoría o logs, además de una inadecuada segregación de funciones, los resultados de la encuesta lo confirman, ilustrando con los virus, la instalación de software no autorizado y los caballos de Troya, que el área de seguridad de la información debe alinear sus esfuerzo para no sólo instalar tecnologías de protección, sino comprender las implicaciones de negocio y los atributos de seguridad, requeridos en los mismos.

Identificación de las fallas de seguridad informática

	2009%	2010%
Material o datos alterados	24,6	11,93
Análisis de registros de auditoría/sistema de archivos/registros Firewall	**47,7**	**23,86**
Sistema de detección de intrusos	**36,0**	**17,95**
Alertado por un cliente/proveedor	23,7	10,12
Alertado por un colega	19,2	10,84

Seminarios o conferencias Nacionales e internacionales	2,7	2,35
Notificación de un empleado/Colaborador	**37,8**	**23,68**

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 advierte que las organizaciones confirman a través de la atención de incidentes la claridad y el nivel real de gestión y generación de valor, que exige el negocio del área de seguridad. El análisis detallado de registros en los sistemas, es una habilidad requerida para detallar lo que ha ocurrido.

Notificación de un incidente de seguridad informática

	2009 %	2010 %
Asesor legal	19,5	17,23
Autoridades locales/regionales	10,8	8,30
Autoridades nacionales(Dijín, Fiscalía)	10,2	5,53
Equipo de atención de incidentes	35,7	41,23
Ninguno: No se denuncian	**39,3**	**27,69**

Comentarios generales:

Las cifras muestran un importante aumento de los equipos de atención de incidentes en la región, sugiriendo una mejor preparación de las organizaciones frente a las fallas que se puedan presentar. Sin embargo, se advierte una porción importante de no denuncia, que envía un mensaje contradictorio y falto de interés, el cual anima a la delincuencia organizada a continuar avanzando, generando miedo y zozobra entre los nuevos ciudadanos de la sociedad de la información y el conocimiento.

Si decide no denunciar

	2009%	2010%
Pérdida de valor de accionistas	9,6	9,17
Publicación de noticias desfavorables en los medios/pérdida de imagen	28,5	**30,17**
Responsabilidad legal	22,5	18,04
Motivaciones personales	25,8	21
Vulnerabilidad ante la competencia	23,4	21,59

Comentarios generales:

El manejo de la imagen y la reputación de la empresa frente a posibles fallas o pérdidas en 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 2010, muestra que las empresas deben concentrarse en la protección de sus datos y en las inversiones basadas en los riesgos de la seguridad, 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

No. de pruebas de seguridad realizadas

	2009%	2010%
Una al año	**30,3**	**30,3**
Entre 2 y 4 al año	29,1	26,74
Más de 4 al año	14,7	9,11
Ninguna	25,9	20,36
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 20,3% no hace ningún esfuerzo en tal sentido. Estas cifras deben llevarnos a meditar en la inseguridad de la información, que constantemente cambia y despeja posibilidades a través de las cuales los intrusos pueden materializar sus acciones. Las pruebas no van a agotar la imaginación ni los medios utilizados por los atacantes para vulnerar las infraestructuras, pero sí muestran un panorama de lo que pueden hacer y contribuyen a destruir el síndrome de la “falsa sensación de seguridad”. Por lo tanto, no prestar la debida atención a tales asuntos, es arriesgarse a formar parte de las estadísticas de los grupos para quienes la seguridad es sólo un referente tecnológico.

Mecanismos de seguridad

	2009 %	2010 %
Smart Cards	14,4	2,25
Biométricos (huella digital, iris, etc.)	25,6	2,63
Antivirus	**86,3**	**11,04**
Contraseñas	**81,9**	**10,92**
Cifrado de datos	48,8	6,45
Filtro de paquetes	31,6	4,75

Firewalls Hardware	57,2	**8,32**
Firewalls Software	**62,5**	7,43
Firmas digitales/certificados digitales	32,5	5,31
VPN/IPSec	50	**8,03**
Proxies	49,1	6,50
Sistemas de detección de intrusos - IDS	36,3	4,08
Monitoreo 7x24	29,7	3,27
Sistemas de prevención de intrusos - IPS	25,9	4,16
Administración de logs	35,6	4,37
Web Application Firewalls	25,9	3,23
ADS (Anomaly detection systems)	6,3	0,97
Herramientas de validación de cumplimiento con regulaciones internacionales	8,8	1,18
Otros: tokens, cifrado de discos, herramientas de análisis de riesgos	-	0,42

Comentarios generales:

Las cifras en 2010 muestran los antivirus, las contraseñas y las VPN como los mecanismos de seguridad más utilizados, seguidos por los sistemas firewalls de software. Dichas tendencias son complementarias con los resultados de la 12th Encuesta de seguridad de Ernst & Young 2010, en la que la inversión se concentra en el mejoramiento de los análisis de riesgos de seguridad de la información, implementación de tecnologías de Data Leakage Prevention – DLP- y programas de concientización en seguridad de la información. Este último informe confirma lo ya expresado por el estudio de Deloitte & Touche 2010, sobre un incremento en la sofisticación de las amenazas a la seguridad de la información, como una de las barreras clave en el aseguramiento del programa de protección de la información.

¿Cómo se entera de las fallas de seguridad?

	2009%	2010%
Notificaciones de proveedores	36,3	21,05
Notificaciones de colegas	43,1	20,25
Lectura de artículos en revistas especializadas	**58,4**	**28,7**
Lectura y análisis de listas de seguridad (BUGTRAQ, SEGURINFO, NTBUGTRAQ, etc.)	49,1	22,64
No se tiene este hábito.	16,6	7,33

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 sugiere un cambio importante para dedicar un espacio en la agenda orientado a la comprensión y revisión de las fallas de seguridad y su impacto en la organización. SEGURINFO, se consolida 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%
No se tienen políticas de seguridad definidas	24,40	14,85
Actualmente se encuentran en desarrollo	**41,60**	**43,84**
Política formal, escrita documentada e informada a todo el personal	34,10	41,30

Comentarios generales:

Revisando la información del año anterior, vemos que el 58,7% de las empresas en Latinoamérica no cuentan con una política de seguridad definida formalmente o se encuentra en desarrollo. Este resultado muestra un ligero avance en el reconocimiento de la información, como un activo fundamental de la organización. Así las cosas y considerando que el informe de Deloitte 2010 se ajusta a lo comentado en esta sección, indicando que una de las mayores barreras en el aseguramiento de la información es la falta de presupuesto (en las empresas de tecnología, medios y telecomunicaciones –TMT), esto no puede ser excusa para no fortalecer el entendimiento de los riesgos de la información, en los diferentes flujos de información en los procesos de negocio.

Principal obstáculo para desarrollar una adecuada seguridad

	2009%	2010%
Inexistencia de política de seguridad	10,40	13,04
Falta de tiempo	12,70	13,4
Falta de formación técnica	10,10	4,71
Falta de apoyo directivo	**18,50**	15,21
Falta de colaboración entre áreas/departamentos	14,00	10,86
Complejidad tecnológica	7,50	9,78
Poco entendimiento de la seguridad informática	14	**18,47**
Poco entendimiento de los flujos de la información en la organización	4,20	5,79

Otras respuestas:	-	8,74

Comentarios generales:

El poco entendimiento de la seguridad informática, la falta de apoyo directivo y el poco tiempo asignado son los rubros más sobresalientes en esta sección. Si bien el año anterior, la tendencia marcaba la baja prioridad del tema en las agendas directivas, este año muestra que no existe el entendimiento suficiente para comprender cómo se mitigan los riesgos de la información, con las medidas de seguridad tecnológicas implementadas. Este resultado es una alerta sobre el lenguaje utilizado para presentar el tema y la necesidad de traducirlo en una expresión natural de la dinámica de los negocios.

Contactos para seguir intrusos

Respuesta	2009%	2010%
No	**52,9**	**50,36**
No Sabe	37,7	35,50
Si, ¿Cuáles?	9,4	14,13

Comentarios generales:

Si por un lado no se denuncian las posibles fallas de seguridad de la información o delitos donde las tecnologías de información son parte fundamental de las conductas punibles, es clara la ausencia de contactos para avanzar en su judicialización y sus infractores, bien sea por desconocimiento o por el riesgo de imagen que implica para la organización. Adicionalmente, frente a 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 infractor, toda vez que, por lo general, 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, uno de los movilizadores más importantes de la seguridad es la continuidad de negocio y la recuperación ante desastres. En este sentido, los gremios, el Gobierno, los proveedores y los usuarios deben organizarse para enfrentar el crimen organizado que busca impactar de manera crítica las infraestructuras tecnológicas, mediante engaños o ataques, lo que exige de cada uno de los actores, una postura de seguridad resiliente que, no es otra cosa que una recuperación proactiva y progresiva, frente a cualquier falla parcial o total de las medidas de seguridad o sistemas de información.

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

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

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

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 permiten a la organización ordenar la práctica de dichas áreas. Este resultado contrasta con lo expuesto en el informe de Ernst & Young 2010, donde se identifica que las organizaciones, a la fecha, no tienen un sistema de gestión de seguridad de la información, pero están considerando hacerlo en el futuro próximo.

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 alguna regulación, muestran 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 accionarios, para generar un esfuerzo común, en procura de una cultura de seguridad de la información más homogénea y dinámica.

CAPITAL INTELECTUAL

No. de personas dedicadas a seguridad informática

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

Comentarios generales:

Los resultados muestran que en Latinoamérica existe un número reducido de personas dedicadas de tiempo completo a los tema de seguridad de la información, bien sea por el tamaño de las organizaciones o por las prioridades actuales de las organizaciones. Así mismo, se nota una disminución importante de empresas que no cuentan con profesionales dedicados a los temas de seguridad informática, hecho que sugiere una mayor apropiación del tema en las diferentes industrias que participaron.

Años de experiencia requeridos para trabajar en seguridad informática

	2009 %	**2010 %**
Ninguno	21,5	3,34
Menos de un año de experiencia	11,8	5,47
Uno a dos años	29	28,57
Más de dos años de experiencia	**37,7**	**44,07**
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 la aplicación 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 en

seguridad informática en la región, con relación al 3,34%, donde se no se exige ninguna experiencia.

Certificaciones en seguridad informática

	2009 %	2010 %
Ninguna	**57,9**	**37,23**
CISSP - Certified Information System Security Professional	20,5	16,4
CISA - Certified Information System Auditor	13,8	14,3
CISM - Certified Information Security Manager	11,8	**13,5**
CFE - Certified Fraud Examiner	4	2,34
CIFI - Certified Information Forensics Investigator	4	3,1
CIA - Certified Internal Auditor	8,4	4,68
SECURITY+	8,4	4,68
GIAC-SANS	-	2,86
NSA IAM/IEM	-	0,78

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 en esa dirección. Se observa poca oferta de formación académica en el tema, certificaciones como CISSP, CISA y CISM marcan una tendencia y preferencia entre los profesionales latinoamericanos que se dedican a los temas de seguridad de la información.

Certificaciones en seguridad informática requeridas para ejercer la función de seguridad

	2010
CISSP - Certified Information System Security Professional	**23,36%**
CISA - Certified Information System Auditor	**14,67%**
CISM - Certified Information Security Manager	**17,39%**
CFE - Certified Fraud Examiner	4,78 %
CIFI - Certified Information Forensics Investigator	**8,04**%
CIA - Certified Internal Auditor	6,86%
MCSE/ISA-MCP (Microsoft)	5,65%
Unix/Linux LP1	5,65%
Security+	**7,28%**

NSA IAM/IEM	2,06

Comentarios generales:

Esta pregunta nos muestra 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, Security+ y CIA que, aunque no aparecen 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
Están ofreciendo programas académicos formales en esta área	**22,38**
Existen limitados laboratorios e infraestructura para soportar los cursos especializados	3,73
Hacen poca difusión sobre éstos temas	5,59
Hay poca investigación científica en el área	4,85
Hay poca motivación de los estudiantes para estudiar el tema	1,11
Hay poca oferta (o nula) de programas académicos en esta área	**26,11**
Hay pocas (o nulas) alianzas con proveedores de tecnología de seguridad y/o agremiaciones relacionadas con el tema	2,61
La formación es escasa y sólo a nivel de cursos cortos	**15,67**
Los estudiantes no conocen las oportunidades laborales en esta área	2,98
Los profesores tienen poca formación académica en el tema	4,10
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

Comentarios generales:

Este año se incluye esta pregunta con el fin de evidenciar el papel de la educación superior en la formación de profesionales en seguridad de la información. Este primer resultado advierte una contradicción; en cuanto a los participantes se dividen entre una poca oferta de programas académicos (26,1%) y la existencia de programas formales (22,3%). Lo que este resultado nos sugiere es que aún no se consolida la Academia como el escenario natural de la formación de los profesionales de la seguridad de la información. Recuperar el liderazgo en esta área, que la industria y la práctica han consolidado con el paso de los años, no será tarea fácil. 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. 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 alguna regulación, muestran que los esfuerzos nacionales en seguridad de la información son parciales y sectorizados, por ejemplo en el sector financiero.
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 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. Se advierte un particular interés en las certificaciones CIFI, Security+ y CIA que aunque no aparecen referenciadas con altos porcentajes, sí son consideradas importantes por la industria.
4. Latinoamérica sigue una tendencia de la inversión en seguridad concentrada en temas perimetrales, las redes y sus componentes, así como en 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 proceso de negocio.
5. Las cifras en 2010 muestran los antivirus, las contraseñas y las VPN como los mecanismos de seguridad más utilizados, seguidos por los sistemas firewalls de software. Existe un marcado interés por las herramientas de prevención de fuga de información.
6. La limitada aplicación de las normas o regulaciones vigentes en temas de delito informático en Latinoamérica y los detallados procedimientos probatorios requeridos para adelantar un dictamen técnico, puede resultar más costoso para la organización que para el posible infractor, toda vez que la carga de la prueba, por lo general, está a cargo de la parte afectada y los posibles costos derivados de peritaje informático o análisis forenses, no ayudan con la economía procesal requerida.

7. Si bien están tomando fuerza las unidades especializadas en delito informático en Latinoamérica, es necesario continuar desarrollando esfuerzos conjuntos entre la Academia, el Gobierno, las organizaciones y la industria, para mostrarles a los intrusos que estamos preparados para enfrentarlos.
8. El poco entendimiento de la seguridad informática y la falta de apoyo directivo, 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 sugieren que en Latinoamérica el ISO 27000, ITIL y el Cobit 4.1 son el estándar y las buenas prácticas que están en las áreas de seguridad de la información o en los departamentos de tecnologías de información.
10. Se advierte una contradicción en cuanto a las respuestas de los participantes, frente al papel de la Academia en la formación de profesionales de la seguridad de la información: poca oferta de programas académicos (26,1%) y la existencia de programas formales (22,3%). Lo que este resultado nos sugiere es que aún no se consolida la Academia como el escenario natural de la formación de los profesionales en seguridad de la información.

Referencias

[1] ERNEST & YOUNG (2010) *12th Annual Global Information Security Survey.* Disponible en:http://www.ey.com/Publication/vwLUAssets/12th_annual_GISS/$FILE/12th_annual_GISS.pdf (Consultado: 06-06-2010).
[2] PRICEWATERHOUSECOOPERS (2010) *Global State of Information Security Survey 2010.* Disponible en: http://www.pwc.com/en_GX/gx/information-security-survey/pdf/pwcsurvey2010_report.pdf (Consultado: 06-06-2010).
[3] DELOITTE & TOUCHE (2010) *2010 TMT Global Security Study.* Disponible en: http://www.deloitte.com/assets/Dcom-Global/Local%20Assets/Documents/TMT/2010_TMT_Global_Security_study.pdf (Consultado: 06-06-2010).
[4] FORRESTER (2010) *The state of Enterprise IT Security and emerging trends: 2009 to 2010.* Disponible en: http://www.thesecuritypub.com/wp-content/uploads/Data/state_of_enterprise_it_security_and_emerging.pdf (Consultado: 06-06-2010).

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