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.