

# Seguridad de la Información en Latinoamérica Tendencias 2009<sup>1</sup>

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

## Introducción

Como fruto de la necesidad por conocer la evolución de la seguridad de la información en Latinoamérica y como parte de la estrategia de exploración y descubrimiento de nuestro continente, la Asociación Colombiana de Ingenieros de Sistemas (ACIS), la Universidad del Valle de Atemajac UNIVA en México y el Centro de Atención de Incidentes de Seguridad Informática y Telecomunicaciones ANTEL de Uruguay, han unido esfuerzos con el fin de tomar una primera radiografía al estado actual de la seguridad de la información en el continente.

El análisis presentado a continuación se desarrolló basado en una muestra aleatoria de profesionales de tecnologías de información de Argentina, Chile, Colombia, México, Uruguay y otros países de Latinoamérica,

la cual respondió 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, se ha realizado un conjunto de análisis básicos, los cuales pretenden ofrecer los elementos más sobresalientes de los resultados obtenidos que orienten al lector sobre las tendencias identificadas en el estudio.

Con esto en mente y considerando otros estudios internacionales como el 2009 Annual Global Security Survey de Deloitte and Touche, el *Emerging Cyber Threats Report for 2009* realizado por el Georgia Tech Information Security Center, el Informe de Amenazas de McAfee: Primer semestre del 2009, se procederá a analizar los resultados de la Encuesta

Latinoamericana de Seguridad de la Información 2009.

## Estructura 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 sectores que participan, el tamaño de la organización, el personal dedicado de tiempo completo al área de seguridad, las certificaciones en seguridad, la experiencia requerida para laborar en seguridad, la dependencia organizacional de la seguridad, los cargos de las personas que respondieron las preguntas y su ubicación geográfica.

## Presupuestos

Esta parte muestra si las organizaciones han destinado un rubro para la seguridad informática. Permite re-

visar 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, identificar 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; las buenas prácticas o estándares que utilizan; los contac-

tos nacionales e internacionales para seguir posibles intrusos.

## Capital intelectual

En este grupo interesa conocer la demanda del profesional en Seguridad Informática y la importancia que tiene para las organizaciones las certificaciones en este tema.

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

## Participación por países

	%
Argentina	5.46%
Chile	7.41%
<b>Colombia</b>	<b>55.36%</b>
México	10.33%
Uruguay	6.04%
Otro	15.40%

## Comentarios Generales:

Para el desarrollo de esta primera aproximación a la seguridad de la información en Latinoamérica participaron 513 profesionales en tecnologías de información y carreras afines, donde Colombia presenta la más alta participación en la misma con un

55.36%, que son aproximadamente 284 personas.

## Demografía

### Sectores participantes:

	%
<b>Servicios Financieros y Banca</b>	11,7
<b>Construcción / Ingeniería</b>	4,34
<b>Telecomunicaciones</b>	<b>13,6</b>
<b>Sector de Energía</b>	2,4
<b>Salud</b>	3,2
<b>Alimentos</b>	1,2
<b>Educación</b>	<b>13,6</b>
<b>Gobierno / Sector público</b>	<b>12,3</b>
<b>Manufactura</b>	3,8
<b>Consultoría Especializada</b>	12,3

### Comentarios Generales:

Los resultados muestran una participación activa del sector de las telecomunicaciones, el sector educativo, el gobierno y 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 y una demanda creciente por el

cumplimiento de buenas prácticas y referentes internacionales.

### No. De Empleados de la Organización

	%
1 a 50	31
51 a 100	7,3
101 a 200	8,5
201 a 300	5,1
301 a 500	7,5
501 a 1000	9,1
<b>Mas de 1000</b>	<b>31,4</b>

### 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 elemento diferenciador y generador de confianza y valor para la empresa, sus clientes y grupos de interés. Las empresas en Latinoamérica muestran un claro interés para formular estrategias de protección de la información que les permita participar en un contexto interconectado y global.

### Dependencia organizacional del área de seguridad informática

	%
Auditoria interna	5,1

Director de Seguridad Informática	21,9
<b>Director Departamento de Sistemas/Tecnología</b>	<b>36,8</b>
Gerente Ejecutivo	1,4
Gerente de Finanzas	0,4
Gerente de Operaciones	2,2
No se tiene especificado formalmente	20,9

### 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. En este sentido, se advierte un marcado interés técnico de la seguridad, que si bien se basa en un reconocimiento de los riesgos asociados con la información, no trasciende de manera formal a los procesos de negocio, donde debería estar inmersa como parte esencial de su diseño y operación.

### Cargos que respondieron la encuesta

	%
Presidente/Gerente General	6,5
Director Ejecutivo	3,0
Director/Vicepresidente	2,8

Director/Jefe de Seguridad Informática	6,9
Profesional del Departamento de Seguridad Informática	11,9
<b>Profesional de Departamento de Sistemas/Tecnología</b>	<b>33,2</b>
Asesor externo	4,7
Auditor Interno	8,7

### **Comentarios Generales:**

Los resultados de esta primera encuesta confirman que son los profesionales de tecnologías de información, quienes están en la infraestructura y operación fueron los que más participaron en esta iniciativa; siguiendo de manera preferente aquellos ubicados formalmente en las áreas de seguridad informática creadas en las organizaciones. Estos datos nos ilustran que se requiere un nivel de madurez de la función de seguridad de la información que le permita ser más que un aliado tecnológico del negocio, un socio estratégico que genere valor para la organización y sus clientes.

### **Presupuesto**

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

	%
<b>Protección de la red</b>	<b>74,4</b>
Proteger los datos críticos de la organización	57,9
Proteger la propiedad intelectual	23,1
Proteger el almacenamiento de datos de clientes	44,9
Concientización/formación del usuario final	26,7
Comercio/negocios electrónicos	16,2
Desarrollo y afinamiento de seguridad de las aplicaciones	25,1
Seguridad de la Información	53,1
Contratación de personal más calificado	15,1
Evaluaciones de seguridad internas y externas	29,2
Pólizas contra cibercrimen	6
Cursos especializados en seguridad informática(cursos cortos, diplomados, especializaciones, maestrías)	21,3
Cursos de formación de usuarios en seguridad informática	12,6
Monitoreo de Seguridad Informática 7 x 24	27,7

## Comentarios Generales:

Latinoamérica muestra una tendencia en la inversión en seguridad concentrada en temas perimetrales, las redes y sus componentes, así como la protección de datos de clientes que se reafirma con el 53,1% en temas de seguridad de la información. Si estos datos son correctos la función de seguridad de la información, si bien está concentrada en los temas tecnológicos, existe un marcado interés por el aseguramiento de los flujos de información en la organización, que nos dice que la administración de riesgos de tecnología comienza a tomar un rumbo más hacia el negocio y sus impactos. Estos datos, son consistentes con los resultados expuestos en el 2009 Annual Global Security Survey de Deloitte and Touche, donde la función de seguridad se mueve de un entorno tecnológico de operación a uno de riesgos, generalmente animado por cumplimiento de regulaciones y normas internacionales.

## Presupuesto previsto para Seguridad Informática 2009

	%
<b>Menos de USD\$50.000</b>	<b>50,3</b>
Entre USD\$50.001 y USD\$70.000	17,4
Entre USD\$70.001 y USD\$90.000	6,90

Entre USD\$90.001 y USD\$110.000	6,20
Entre USD\$110.001 y USD\$130.000	4,4
Más de USD\$130.000	14,9

## Comentarios Generales:

Si bien las exigencias de nuevos marcos regulatorios 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 las 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

	%
Ninguno	8,1
Manipulación de aplicaciones de software	22,2
<b>Instalación de software no autorizado</b>	<b>60,7</b>

Accesos no autorizados al web	30,9
Fraude	10,8
<b>Virus</b>	<b>70,9</b>
Robo de datos	9,9
<b>Caballos de troya</b>	<b>33</b>
Monitoreo no autorizado del tráfico	11,4
Negación del servicio	15
Pérdida de integridad	4,8
Pérdida de información	19,5
Suplantación de identidad	13,5
Phishing	16,8
Pharming	3
Fuga de Información	21

### **Comentarios Generales:**

Mientras en el informe de Deloitte and Touche de 2009 se muestran claramente que los hallazgos más frecuentes identificados por la auditoría en el ejercicio de seguimiento y verificación son exceso de privilegios, inadecuada segregación de funciones y incumplimiento de procedimientos de control de acceso, los resultados de la encuesta confirman éstos 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 solamente instalar tecnologías de protección, sino com-

prender las implicaciones de negocio y los atributos de seguridad requeridos en los mismos.

### **Identificación de las fallas de seguridad informática**

	%
Material o datos alterados	24,6
<b>Análisis de registros de auditoría/sistema de archivos/registros Firewall</b>	<b>47,7</b>
<b>Sistema de detección de intrusos</b>	<b>36,0</b>
Alertado por un cliente/proveedor	23,7
Alertado por un colega	19,2
Seminarios o conferencias Nacionales e internacionales	2,7
<b>Notificación de un empleado/Colaborador</b>	<b>37,8</b>

### **Comentarios Generales:**

Los registros de auditoría cada vez más adquieren importancia en el ejercicio de la función de seguridad de la información. En este contexto, se advierte que las organizaciones comienzan a comprender que sólo mediante al atención de incidentes se hace claro y real el nivel de gestión y generación de valor que exige el negocio del área de seguridad. La participación de los colaboradores es la fuente de mayor información sobre

el análisis de la situación que se ha presentado. El intercambio de experiencia a través de listas de seguridad en Latinoamérica es una tendencia emergente.

### **Notificación de un incidente de seguridad informática**

	%
Asesor legal	19,5
Autoridades locales/ regionales	10,8
Autoridades nacionales(Dijín, Fiscalía)	10,2
Equipo de atención de incidentes	35,7
<b>Ninguno: No se denuncian</b>	<b>39,3</b>

### **Comentarios Generales:**

Estas cifras confirman lo que intuitivamente se comenta en los diferentes foros de seguridad de la información en Latinoamérica: no existe una clara cultura de reporte, lo que envía un mensaje de falta de interés y preparación para enfrentar a las bandas delincuenciales y grupos de cibercriminales emergentes, quienes aprovechándose del miedo propio de la pérdida de imagen, la falta de oportunidad y celeridad en la judicialización de los delitos informáticos, se fortalecen y mimetizan a través de

las actividades diarias de las organizaciones.

### **Si decide no denunciar**

	%
Pérdida de valor de accionistas	9,6
<b>Publicación de noticias desfavorables en los medios/pérdida de imagen</b>	<b>28,5</b>
Responsabilidad legal	22,5
Motivaciones personales	25,8
Vulnerabilidad ante la competencia	23,4

### **Comentarios Generales:**

Los responsables de la seguridad de la información deben mantener un nivel de evaluación y control sobre los objetos y elementos susceptibles de ser vulnerados. En este orden de ideas la administración de riesgos de seguridad articulados con aquellos identificados para los procesos de negocio, deben ser un imperativo que produzca sistemas de gestión de seguridad y de proceso más resistente, resiliente y confiable. Si esto es correcto y se aplica de manera sistemática y sistémica en la dinámica de negocio de la organización, las denuncias de incidentes no deberían impactar la imagen de las empresas, al contrario, debería fortalecerlas y reconocerlas



por su compromiso con el cliente y su propio gobierno

## Herramientas y prácticas de seguridad

### No. De pruebas de seguridad realizadas

	%
<b>Una al año</b>	<b>30,3</b>
Entre 2 y 4 al año	29,1
Más de 4 al año	14,7
Ninguna	25,9
Vulnerabilidad ante la competencia	23,4

### 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 25,9 % no hace ningún esfuerzo en este 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 si nos dan un panorama de lo que pueden hacer y nos ayudan a evitar 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 referente tecnológico que hay que tener.

### Mecanismos de Seguridad

	%
Smart Cards	14,4
Biométricos (huella digital, iris, etc.)	25,6
<b>Antivirus</b>	<b>86,3</b>
<b>Contraseñas</b>	<b>81,9</b>
Cifrado de datos	48,8
Filtro de paquetes	31,6
Firewalls Hardware	57,2
<b>Firewalls Software</b>	<b>62,5</b>
Firmas digitales/certificados digitales	32,5
VPN/IPSec	50
Proxies	49,1
Sistemas de detección de intrusos - IDS	36,3
Monitoreo 7x24	29,7
Sistemas de prevención de intrusos - IPS	25,9
Administración de logs	35,6
Web Application Firewalls	25,9
ADS (Anomaly detection systems)	6,3

Herramientas de validación de cumplimiento con regulaciones internacionales	8,8
---	-----

### Comentarios Generales:

Las cifras en 2009 muestran a los antivirus, las contraseñas y los firewalls de software como los mecanismos de seguridad más utilizados, seguidos por los sistemas VPN y proxies. Dichas tendencias son coherentes como estrategias contra amenazas críticas como el ciberterrorismo, la manipulación de páginas web, negación del servicio y brechas de exposición de datos reportada tanto en el informe de amenazas del Georgia Tech Information Security Center como en el de Deloitte and Touche. En este último informe se muestra un marcado interés por las herramientas de cifrado de datos y control de contenidos dos tendencias emergentes ante las frecuentes fugas de información y migración de las aplicaciones web al contexto de servicios o web services.

### ¿Cómo se entera de las fallas de seguridad?

	%
Notificaciones de proveedores	36,3
Notificaciones de colegas	43,1

<b>Lectura de artículos en revistas especializadas</b>	<b>58,4</b>
Lectura y análisis de listas de seguridad (BUGTRAQ, SEGURINFO, NTBUGTRAQ, etc.)	49,1
No se tiene este hábito.	16,6

### 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. Si bien 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 para la comprensión y revisión de las fallas de seguridad y su impacto en la organización. SEGURINFO, continúa creciendo llegando en este momento a 2000 participantes desde su fundación en el año 2000.

### Políticas de seguridad

#### Estado actual de las políticas de seguridad

	%
No se tienen políticas de seguridad definidas	24,40
<b>Actualmente se encuentran en desarrollo</b>	<b>41,60</b>

Política formal, escrita documentada e informada a todo el personal	34,10
---	-------

### **Comentarios Generales:**

El 66% de las empresas en Latinoamérica no cuentan con política de seguridad definidas formalmente o se encuentran en desarrollo. Esta cifra muestra que si bien se ha avanzado 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 cómo 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**

	%
Inexistencia de política de seguridad	10,40%
Falta de tiempo	12,70%
Falta de formación técnica	10,10%
<b>Falta de apoyo directivo</b>	<b>18,50%</b>

Falta de colaboración entre áreas/ departamentos	14,00%
Complejidad tecnológica	7,50%
Poco entendimiento de la seguridad informática	14
Poco entendimiento de los flujos de la información en la organización	4,20%

### **Comentarios Generales:**

La falta de apoyo directivo, la poca colaboración entre las áreas y el poco tiempo asignado al tema se manifiestan como los rubros más sobresalientes en esta sección. Estas cifras hablan del limitado entendimiento de la seguridad de la información en el contexto de negocio, de la poca creatividad de los profesionales de la seguridad 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. La gestión de la seguridad de la información entendida más allá del PHVA (Planear, Hacer, Verificar y Actuar) del ISO 27001, es construir un lenguaje común de negocios que vea en la seguridad una forma de integrarse con la dinámica del mundo globalizado.

### **Contactos para seguir intrusos**

<b>No</b>	<b>52,9</b>
No Sabe	37,7
Si, ¿Cuáles?	9,4

### **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 claro que no se tengan contactos para avanzar en la judicialización de éstas y sus infractores, bien sea por desconocimiento 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, dado 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.

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 resilientes frente a los embates de la inseguridad de la in-

formación. Adicionalmente se hace necesario establecer acuerdos interinstitucionales e internacionales con entes de policía judicial para actuar con oportunidad frente a una conducta punible en medios informáticos.

### **Estándares y buenas prácticas en seguridad Informática y Regulaciones en seguridad de la información**

<b>Estándares y buenas prácticas</b>	<b>%</b>
<b>ISO 27001</b>	<b>45,8</b>
Common Criteria	5,2
Cobit 4.1	23,4
Magerit	5,2
Octave	2,3
Guías del NIST (National Institute of Standards and Technology) USA	12,3
Guías de la ENISA (European Network of Information Security Agency)	2,3
Top 20 de fallas de seguridad del SANS	7,1
OSSTM - Open Standard Security Testing Model	7,5
ISM3 - Information Security Management Maturiy Model	3,9
ITIL	26,9

<b>No se consideran</b>	<b>37,7</b>
-------------------------	-------------

<b>Norma</b>	<b>%</b>
<b>Ninguna</b>	<b>52,30</b>
Regulaciones internacionales (SOX, BASILEA II)	15,60
Normativas aprobadas por entes de supervisión (Superintendencias, Ministerios o Institutos gubernamentales)	33,80

### **Comentarios Generales:**

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 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. En ese mismo sentido, las regulaciones sobre seguridad de la información lideradas por regulaciones internacionales como SOX y Basilea II, en contraste de 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**

	<b>%</b>
Ninguna	34,30
<b>1 a 5</b>	<b>44,10</b>
6 a 10	11,80
11 a 15	3,70
Más de 15	6,10

### **Comentarios Generales:**

Los resultados muestran que en Latinoamérica se tiene un número reducido de personas dedicadas de tiempo completo a los temas de seguridad de la información, esto bien sea por el tamaño de las organizaciones, como por las prioridades que actualmente éstas tienen. Así mismo, se advierte una preocupación importante, cuando se observa un 34,3% donde los participantes dicen que no se tienen profesionales destinados formalmente a esta función. Revisando el entorno de la región, se prevé con el paso del tiempo, que esta situación cambie por la aparición de regulaciones internacionales que obliguen al desarrollo

de un entorno de seguridad y control inherente y sistemático.

### **Años de experiencia requeridos para trabajar en seguridad informática**

	%
Ninguno	21,5
Menos de un año de experiencia	11,8
Uno a dos años	29
<b>Más de dos años de experiencia</b>	<b>37,7</b>

### **Comentarios Generales:**

En la región se muestra una clara tendencia a que aquellos que cuentan con más de dos años de experiencia en temas de seguridad informática son candidatos elegibles para trabajar en las áreas de seguridad. Pese a que en la actualidad, exista una oferta limitada de formación académica en estos temas y que la exposición y aplicación autodidacta frente a los dilemas de seguridad es la constante, no es extraño observar que un 21,5% de las organizaciones no exijan experiencia en el tema, pues por lo general prefieren formarlos internamente a la medida de sus necesidades.

### **Certificaciones en seguridad informática**

	%
Ninguna	57,9
CISSP - Certified Information System Security Professional	20,5
CISA - Certified Information System Auditor	13,8
CISM - Certified Information Security Manager	11,8
CFE - Certified Fraud Examiner	4
CIFI - Certified Information Forensics Investigator	4
CIA - Certified Internal Auditor	8,4
SECURITY+	8,4

### **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 en el hacer de los mecanismos de seguridad tecnológica. Esto ilustra que si bien existe un déficit importante 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 seguridad de la información.

## Importancia de contar con certificaciones en seguridad informática

	Muy Importante	Importante	No es Importante	No sabe
CISSP - Certified Information System Security Professional	44,40%	28,30%	9,30%	17,90%
CISA - Certified Information System Auditor	24,70%	39,00%	16,10%	20,20%
CISM - Certified Information Security Manager	30,70%	37,20%	12,60%	19,50%
CFE - Certified Fraud Examiner	19,70%	31,70%	24,90%	23,70%
CIFI - Certified Information Forensics Investigator	21,40%	28,20%	25,80%	24,60%
CIA - Certified Internal Auditor	16,90%	33,90%	27,00%	22,20%
MCSE/ISA-MCP (Microsoft)	18,90%	28,00%	30,50%	22,60%
Unix/Linux LP1	25,80%	30,10%	23,80%	20,30%
Security+	23,70%	29,40%	19,20%	27,80%

### 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, CISA y CISM 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 con-

tratación. Se advierte un particular interés en las certificaciones CFE, CIA y CIFI que si bien no aparecen con resultados “muy importantes”, si son consideradas importantes por la industria. Las certificaciones son interesantes referentes para la industria frente a las tendencias internacionales, pero se necesita 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 al esquema de certificaciones.

## **Conclusiones generales**

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

1. Las regulaciones internacionales llevarán a las organizaciones en Latinoamérica a fortalecer los sistemas de gestión de la seguridad de la información. Actualmente las normas como SOX y Basilea II comienzan a cambiar el panorama de la seguridad de la información en la Banca y en el mercado accionario.

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. De igual forma, se nota que poco a poco el mercado de especialistas en seguridad de la información toma fuerza, pero aún 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 y formarlos localmente.

3. Las certificaciones CISSP, CISA y CISM 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. Se advierte un importante giro en las certificaciones CFE, CIA y CIFI que si bien no aparecen con resultados “muy importantes”, si son consideradas importantes por la industria.

4. La inversión en seguridad de la información se encuentra concentrada en aspectos perimetrales, las redes y sus componentes, así como la protección de datos de clientes que se reafirma con el 53,1% concentrado en temas de seguridad de la información.

5. Las cifras en 2009 muestran a los antivirus, las contraseñas y los firewalls de software como los mecanismos de seguridad más utilizados, seguidos por los sistemas VPN y proxies. Existe un marcado interés por las herramientas de cifrado de datos y control de contenidos dos tendencias emergentes ante las frecuentes fugas de información y migración de las aplicaciones web al contexto de servicios o web services.

6. La limitada aplicación de las normas o regulaciones vigentes en temas de delito informático en Latinoamérica y baja formación de los jueces en estos temas establece un reto importante para la administración de justicia en el continente. En este contexto, adelantar un proceso jurídico puede resultar más costoso para la organización que para el posible infractor, dado 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 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. La falta de apoyo directivo y la falta de tiempo, 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. La decisión está en sus manos.

9. Los resultados sugieren que en Colombia 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. 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. Así mismo, se manifiesta la necesidad de adelantar al menos un ejercicio anual de análisis de riesgos como soporte a los temas de seguridad y procesos de negocio.

### Pies de página

*<sup>1</sup>Agradecimientos especiales al Ing. Mauricio González, Webmaster y Administrador de la Red de ACIS por su apoyo durante el desarrollo y compilación de resultados de la encuesta.*

### Referencias

[1] MCAFEE (2009) Informe de amenazas. Primer trimestre de 2009.

[2] GEORGIA TECH INFORMATION SECURITY CENTER (2009) Emerging Cyber Threats Report for 2009

[3] DELOITTE & TOUCHE (2009) Annual Global Security Survey

#### Sobre el Autor:

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