Seguridad Informática en Colombia Tendencias 2008[1]

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

Este año la participación en la VIII Encuesta Nacional de Seguridad Informática ascendió a 202 personas de los diferentes sectores productivos del país en el tema de seguridad de la información. En esta ocasión, como en el año anterior se ha vinculado la Universidad del Valle de Atemajac – UNIVA en México, entidad que ha querido adelantar este mismo ejercicio en dicho país, cuyos resultados estarán disponibles en el sitio web de la mencionada institución.

El análisis presentado a continuación se desarrolló basado en una muestra aleatoria que 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 realizó un conjunto de análisis básicos, con el propósito de 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 *2007 Global State of Information Security Study de Pricewaterhousecoopers* – PwC; el *2008 Information Security Breaches Survey* realizado en conjunto con PwC, Hewlett Packard y Symantec; el *2007 Privacy and data protection survey* de Deloitte and Touche; el *CSI Computer Crime and Security Survey* 2007; y, el *IBM X-Force 2007 Trend Statistics* se procederá a analizar los resultados de la Encuesta Nacional de Seguridad Informática ACIS 2008.

Estructura de la encuesta

Fue diseñado un cuestionario compuesto por 31 preguntas sobre los siguientes temas:

- Demografía
- Presupuestos
- Fallas de seguridad
- Herramientas y prácticas de seguridad
- Políticas de seguridad

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 revisar el tipo de tecnología en el que invierten y un estimado del monto de la inversión en seguridad informática.

Fallas de seguridad

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

Herramientas y prácticas de seguridad informática

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

Políticas de seguridad

Finalmente, esta sección busca indagar sobre la formalidad de las políticas de seguridad en la organización; los principales obstáculos para lograr una ade-

cuada seguridad; la buenas prácticas o estándares que utilizan; los contactos nacionales e internacionales para seguir posibles intrusos.

Consideraciones muestrales

Considerando una población limitada (alrededor de 1800 personas que participan activamente en la lista de seguridad SEGURINFO) se ha estimado un error muestral de 7% (confianza del 93%), lo cual nos permite manejar una muestra adecuada cercana a los 183 participantes. Al contar con 202 participantes en la muestra, los resultados presentados son estadísticamente representativos.

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

Demografía

Sectores participantes

	2002 (%)	**2003 (%)**	**2004 (%)**	**2005 (%)**	**2007 (%)**	**2008 (%)**
Banca	10,4	12,5	9,6	13	16,1	16,26
Ingeniería	6,5	2,3	6,4	4	7,3	6,90
Industria Informática/ TI	23,4	13,6	15,1	15	10,8	0
Educación	19,5	19,3	14,2	24	17,6	14,78
Servicios Públicos/Energía	3,9	5,7	1,8	3	1,5	0
Gobierno	16,9	25	10,5	9	16,1	9,85
Seguros	2,6	8	2,7	8	0	0
Petróleo	0	0	1,4	0	0	0,49
Transporte	3,9	2,3	0,5	2	1,5	0
Telecomunicaciones	6,5	10,2	10,0	5	2,5	8,37
Farmacéutico	1,3	0	1,4	2	0	0
Sin ánimo de lucro	5,2	1,1	3,7	1	0	0
Manufactura	-	-	-	-	-	3,45
Salud	-	-	-	-	-	2,46
Alimentos	-	-	-	-	-	0,99
[ ] Otro, especifique: Comercializadora, Vigilancia, Salud, Superintendencia, Consultoría, Cementos, Servicios de Seguridad Informática, Consumo	33,8	22,7	22,8	20	35,8	36,45

Comentarios generales:

Los resultados muestran una participación activa de la banca, el sector educativo, el gobierno, y el sector de telecomunicaciones; cuatro sectores donde de acuerdo con las tendencias internacionales se viene manifestando la necesidad de contar con una directriz formal en temas de seguridad de la información. Adicionalmente, es importante anotar la nueva regulación en materia de seguridad informática expedida por la Superintendencia Financiera de Colombia, Circular 052 de 2007, que acelerará los cambios previstos para banca y el sector financiero en general. A la fecha se adelantan importantes esfuerzos en el sector financiero para dar cumplimiento con esta directriz.

No. De Empleados de la Organización

	AÑO 2002%	**AÑO 2003%**
1 a 100	31,4	19
101 a 250	17,6	13,3
251 a 500	10,8	18,1
501 a 1000	11,8	16,2
1001 a 2500	11,8	16,2
2501 a 5000	8,8	11,4
Más de 5000	7,8	5,7

	AÑO 2004%	**AÑO 2005%**	**AÑO 2007%**	**AÑO 2008%**
1 a 50	27,9	28	27,3	31,03
51 a 100	11,6	19	12,9	9,36
101 a 200	13,0	11	7,7	7,39
201 a 300	3,3	5	7,2	7,88
301 a 500	11,2	12	10,8	11,33
501 a 1000	11,6	13	9,3	7,88
más de1000	21,4	13	24,7	25,12

Comentarios generales

Al igual que en años anteriores la mediana y gran industria participan con porcentajes similares en la encuesta. La seguridad de la información, en la mediana empresa, comienza a ser un elemento clave para la formalización de sus estrategias de negocio y en la gran empresa, se hace evidente como un tema que debe ser parte de la gestión misma de la organización, dado que las regulaciones internas y tendencias internacionales establecen referentes que no pueden ser ignorados en un contexto globalizado.

No. De personas dedicadas a Seguridad Informática

	AÑO 2002%	AÑO 2003%	Diferencia Porc.
1 a 10	90,3	90,6	0,3
11 a 20	3,9	6,6	2,7
21 a 50	3,9	1,9	2
Más de 50	0	0,9	0,9
Ninguna	1,9	0	1,9

	AÑO 2004%	AÑO 2005 %	AÑO 2007 %	AÑO 2008 %
Ninguna	26,8	26	28,6	23,65
1 a 5	58,2	58	54,9	62,56
6 a 10	10,9	5	10,9	8,37
11 a 15	0,9	5	0,5	1,97
Más de 15	3,2	6	5,2	3,45

Comentarios generales:

Los resultados de este año sugieren un ligero aumento de las personas dedicadas de tiempo completo a los temas de seguridad (1 a 5 y 11 a 15). Estos dos resultados muestran por un lado, el renovado interés de la mediana empresa por dedicarle recursos al tema de seguridad de la información, el cual implica mayores niveles de confianza en sus clientes y, por otro lado, el incremento de personal en la gran empresa, fruto de las regulaciones nacionales e internacionales que obligan a contar con un nivel mínimo de gestión de seguridad de la información. No deja de preocupar el 23,65% que no tiene ninguna persona dedicada exclusivamente al tema de seguridad, lo que sugiere que existe una porción importante de empresas que están aún sin establecer formalmente recursos a este tema.

Dependencia organizacional del área de seguridad informática

	2002%	2003%	2004%	2005%	2007%	2008%
Auditoría interna	5	3,9	6,1	7	4,8	5,56
Director de Seguridad Informática	11,9	14,7	10,2	18	20,5	25,25
Director Departamento de Sistemas/Tecnología	60,4	52,9	53,8	39	44,6	38,89
Gerente Ejecutivo	4	2	1,5	4	0,6	1,52

Gerente de Finanzas	0	1	1	0	0	2,02
No se tiene especificado formalmente	11,9	22,5	18,3	21	17,5	19,7
Otro, especifique: Riesgo operativo, Vicepresidencia de Operaciones, Jefe de Telemática, etc.	6,9	2,9	9,1	11	12	7,07

Comentarios generales:

Los resultados de este año muestran un aumento significativo del cargo de director de seguridad de la información, con una leve disminución de la dependencia del área de tecnología. De igual forma, se sugiere un moderado incremento de organizaciones que no tienen formalmente especificada la dependencia del tema de seguridad de la información. Según se observa en los datos, la seguridad de la información continúa ganando terreno, pero se hace necesario afinar el discurso tanto de las áreas de seguridad como de tecnología para que sus propuestas se afinen con los procesos de negocio y no estrictamente con los elementos tecnológicos y de infraestructura.

Años de experiencia requeridos para trabajar en seguridad informática

	2007%	**2008%**
Ninguna	6.6	8,39
Menos de un año de experiencia	10,7	7,1
Uno a dos años	38,5	39,9
Más de dos años	44,3	51,61

Comentarios generales:

En este segundo año los resultados para esta pregunta muestran con claridad que la industria en Colombia exige más de dos años de experiencia en seguridad informática como requisito para optar por una posición en esta área. De igual forma, se nota que poco a poco el mercado de especialistas en seguridad de la información toma fuerza, pero aún la oferta de programas académicos formales se encuentra limitada, lo que hace que la experiencia requerida se forme en la práctica misma de la seguridad de la información. En este sentido, no es extraño que exista un 8,39% de empresas que no exijan experiencia en el tema de seguridad de la información, pues prefieren formarlos a la medida de sus necesidades.

Certificaciones en seguridad informática

	2007%	2008%
Ninguna	60,3	36,5
CISSP	20,7	19,2
CISA	14,9	13,3
CISM	9,9	13,8
CFE	0,8	3,94
CIFI	5,8	1,97
CIA	10,7	4,43
Security+	-	5,91
Otras: Especializaciones en Auditoría de Sistemas, Especializaciones en Seguridad Informática, Diplomados en Seguridad Informática, Auditor Líder BS7799, Certified Ethical Hacking, CCNA, CCSP, GSEC, MCSE, etc.	18,2	13,8

Comentarios generales:

Al igual que la pregunta anterior, este segundo año los resultados muestran un alto porcentaje de encuestados que respondieron que no cuentan con certificaciones en temas de auditoría, fraude, seguridad informática o informática forense. Sin embargo, se notan unos ligeros incrementos en la certificación CISM y CFE, certificaciones orientadas a los temas de gerencia de la seguridad de la información y administración y control del fraude respectivamente. Se mantiene un interés por la certificación CISSP. Esto resultados reiteran el llamado a la academia para atender la demanda de formación en estas áreas, que actualmente las organizaciones exigen como un nuevo perfil para fortalecer sus esquemas de seguridad y control de cara a la exigencia de un escenario globalizado.

Importancia de contar con certificaciones en seguridad informática

2007	Muy importante %	Importante%	No es importante%	No sabe%
CISSP	46	39	10	5
CISA	25	38	26	10
CISM	31	49	13	8
CFE	19	37	33	11
CIFI	21	36	31	12

CIA	23	38	26	13
MCSE/ISA-MCP	17	33	34	15
Unix/Linux LP1	23	30	33	14

2008	Muy importante %	Importante %	No es importante%	No sabe%
CISSP	51,03	38,62	3,45	6,90
CISA	25,74	53,68	11,03	9,56
CISM	40,15	44,53	5,84	9,49
CFE	22,9	42,75	19,08	15,27
CIFI	23,62	43,31	22,83	10,24
CIA	16,94	49,19	20,97	12,90
MCSE/ISA-MCP	22,83	37,01	27,56	12,60
Unix/Linux LP1	31,78	37,21	20,93	10,08
Security+	31,78	34,88	14,73	18,60

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 contratación. Se advierte un importante giro en las certificaciones CFE, CIA y CIFI que si bien no aparecen con resultados "muy importantes", sí 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.

Cargos que respondieron la encuesta

	2002 %	2003 %	2004 %	2005 %	2007 %	2008 %
Presidente/Gerente General/Director Ejecutivo	8,5	6,7	9,8	5	7,2	5,56
Director/Vicepresidente	16	8,6	5,2	6	3,6	3,03
Director/Jefe de Seguridad Informática	11,3	15,2	8,2	14	10,2	11,11

Profesional del Departamento de Seguridad Informática	11,3	3,8	8,8	11	12,7	9,60
Profesional de Departamento de Sistemas/Tecnología	35,8	46,7	44,8	36	36,1	36,87
Auditor Interno	2,8	2,9	4,1	4	1,2	5,05
Asesor Externo	-	-	-	-	-	5,05
Otro, especifique: Director de Investigación y Desarrollo, Investigador criminalístico, Gerente de proyectos, Consultor de seguridad.	14,2	16,2	19,1	24	27,1	21,21

Comentarios generales:

Los resultados de este año continúan marcando una seguridad informática dentro del área de tecnologías de información, con un fuerte énfasis en el tema de infraestructura y operación. Un ligero aumento en la participación de los gerentes o directores de seguridad, muestra que este cargo, comienza a tener un lugar importante dentro de la organización.

De igual forma, la participación de la alta gerencia a pesar de ser limitada en los resultados de este año, continúa haciéndose presente y denotando que el tema es de su interés, pero en el contexto del negocio. Nuevamente se insiste en la necesidad de abrir espacios de comunicación bidireccionales entre la gerencia del negocio y la de seguridad de la información, para avanzar en una reflexión coordinada que beneficie tanto a la organización como al área de seguridad.

Presupuesto

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

	2002 %	**2003 %**	**2004 %**	**2005 %**	**2007 %**	**2008 %**
Protección de la red	19,3	22,7	20,6	19	74,1	75,9
Proteger los datos críticos de la organización	19,8	19,5	18,8	18	62	61,1
Proteger la propiedad intelectual	8,9	3,7	6,1	6	21,1	30
Proteger el almacenamiento de datos de clientes	12,8	13,7	11,7	12	47,6	47,8
Concientización/formación del usuario final	7,8	7,4	9,2	8	28,3	33,5
Comercio/negocios electrónicos	4,7	4	6,5	5	10,8	21,2

Desarrollo y afinamiento de seguridad de las aplicaciones	9,4	10,3	8,1	11	27,1	31
Asesores de seguridad informática	5,5	5,8	6,3	7	20,5	23,2
Contratación de personal más calificado	1,8	1,8	2,0	3	13,9	11,3
Evaluaciones de seguridad internas y externas	9,9	9,8	9,6	4	25,9	25,1
Monitoreo de Seguridad Informática 7x24	-	-	-	-	25,3	25,6
Cursos especializados	-	-	-	-	-	25,6
Cursos de formación usuarios en seguridad informática	-	-	-	-	-	15,3
Pólizas de cibercrimen	-	-	-	-	-	4,43
Otro, especifique: Ninguno, Capacitación, auditoría, certificaciones de seguridad, continuidad del negocio	0,3	1,3	1,1	0	27,1	6,4

Comentarios generales:

Los resultados de este año reafirman la tendencia de la inversión en seguridad concentrada en la zona perimetral, en las redes y sus componentes, así como la protección de datos de los clientes y un ligero interés en el tema de control de la propiedad intelectual y derechos de autor. Llama la atención la aparición del tema de pólizas de cibercrimen, un elemento emergente que se empieza a imponer a nivel internacional, como un nuevo control que obliga a las organizaciones a mantener un ejercicio permanente de evaluación, que ofrezca al asegurador mayor confianza frente a su asegurado y por ende, menos implicaciones en los deducibles de la póliza. Estos datos, son consistentes con los resultados expuestos en el 2008 *Information Security Breaches Survey*, adelantado en el Reino Unido con PriceWaterhouseCoopers, Symantec y Hewlett Packard, donde se indican como motivadores clave de la seguridad, proteger la información del cliente, proteger la reputación de la organización y mantener la integridad de los datos.

Presupuesto previsto para Seguridad Informática 2007

	2003 %	**2004 %**	**2005 %**	**2007 %**	**2008 %**
Menos de USD$50.000	64,3	58,1	50	67,9	58,33

Entre USD$50.001 y USD$70.000	12,2	15,2	21	12,7	15,10
Entre USD$70.001 y USD$90.000	3,1	5,7	6	7,3	4,69
Entre USD$90.001 y USD$110.000	3,1	6,7	8	1,8	5,21
Entre USD$110.001 y USD$130.000	4,1	3,8	3	3	4,17
Más de USD$130.000	13,3	10,5	12	7,3	12,50

Comentarios generales:

En 2007 la inversión en seguridad informática muestra un aumento importante en el segmento de USD$130.000, dadas las consideraciones de normas aplicables que exigen medidas y prácticas de seguridad de la información, particularmente en la Banca y en la gran industria. De igual forma, se advierte que el nivel de inversión en la mediana empresa continúa por debajo de los USD$50.000, con un leve descenso en el porcentaje, con relación al año anterior. Esta situación establece un interesante contraste con la cifra siguiente (entre USD$50.001 y USD$70.000) que sugiere un ligero aumento de la inversión en este tema. Este desarrollo de la inversión, con el advenimiento de una dinámica fuerte de la seguridad, animada por la aplicación de norma de la Superintendencia Financiera, puede generar nuevas oportunidades y exigencias en otros sectores que impulsen un mayor nivel de inversión en seguridad de la información en los años venideros.

La encuesta 2007 *Computer Crime and Security Survey*, muestra que las empresas norteamericanas aumentaron ligeramente su inversión en seguridad informática, entre el 3 y 5% del presupuesto total de tecnologías de información; mientras el año anterior se tenían incrementos por encima del 10%. A pesar de las tensiones de los mercados internacionales y las caídas de las principales bolsas del mundo que afectaron las utilidades de las empresas, la inversión en seguridad se mantuvo.

Presupuesto previsto para Seguridad Informática 2008

	2007 %	**2008 %**
Menos de USD$50.000	61,8	50,52
Entre USD$50.001 y USD$70.000	13,3	19,27
Entre USD$70.001 y USD$90.000	4,8	7,29
Entre USD$90.001 y USD$110.000	6,1	5,73
Entre USD$110.001 y USD$130.000	1,8	5,73
Más de USD$130.000	12,1	11,46

Comentarios generales:

Las proyecciones de las organizaciones en los temas de inversión en seguridad sugieren unos incrementos moderados para el 2008, los cuales se orientan fundamentalmente a cumplir con normatividad de obligatorio cumplimiento, certificaciones de procesos de misión crítica y temas de pólizas de seguro, frente a temas de cibercriminalidad. Estas inversiones generalmente desarrolladas por la Banca, el sector de telecomunicaciones y la grande empresa, establecen un referente base para la dinámica empresarial del país, que le dice a cada uno de los sectores productivos que la seguridad de la información no es un tema de los "informáticos" y requiere el concurso de la gerencia y el área de tecnología.

Estas tendencias se confirman en el informe 2007 *Global State of Information Security Study de Pricewaterhousecoopers*, donde se resaltan como motivadores de la inversión en seguridad la continuidad de negocio, el cumplimiento de regulaciones y normativas internas y externas y la protección de la reputación de la empresa. Es interesante comentar que este mismo informe muestra que las organizaciones, en un 39%, adelantan al menos un ejercicio de análisis de riesgos como soporte a los temas de seguridad y procesos de negocio.

Fallas de seguridad

Tipos de fallas de seguridad

	2002 %	**2003 %**	**2004 %**	**2005 %**	**2007 %**	**2008 %**
Ninguno	5,4	8,7	6,6	9	5,3	2,46
Manipulación de aplicaciones de *software*	4,5	4,3	5,8	8	24,8	14,8
Accesos no autorizados al *web*	14,8	10,6	9,4	10	35,4	26,6
Fraude	4	3,9	1,8	5	13,3	6,4
Virus	33,6	33,3	34,9	29	62,8	41,9
Robo de datos	3,6	3,9	2,6	2	10,6	7,39
Caballos de troya	4,9	4,8	10,0	11	29,2	16,7
Monitoreo no autorizado del tráfico	4,9	7,7	5,8	8	7,1	9,36
Negación del servicio	6,3	7,2	7,6	7	21,2	13,8
Pérdida de integridad	6,7	3,9	2,9	3	12,4	4,93
Pérdida de información	9,4	10,1	10,5	7	24,8	11,3
Phising	-	-	-	-	17,7	11,8

Pharming	-	-	-	-	3,5	1,48
Software no autorizado	-	-	-	-	-	40,9
Otros, especifique: pérdida de laptops, acceso no autorizado a equipos, fuga de información, *spyware*.	1,8	1,4	2,1	1	6,2	1,97

Comentarios generales:

Los resultados en esta ocasión nos presentan al código malicioso, el *software* no autorizado y los accesos no autorizados a la *web* como las fallas más frecuentes en Colombia. Estas tendencias se confirman en el IBM Xforce 2007 Trend Statistics donde se establece que:

- A pesar de una disminución del número de vulnerabilidades, hubo un incremento del 28% de ellas que fueron de alta severidad.
- Aumento de la presencia del *Web exploit toolkits*, como herramientas para vulnerar los sitios web y sus aplicaciones de soporte.

Estos datos deben llamar a la reflexión tanto a desarrolladores como a profesionales de la seguridad de la información con el fin de revisar y evaluar el código que desarrollan, así como los procedimientos de instalación y configuración de las herramientas de seguridad respectivamente. Luchar contra la inseguridad de la información no es solamente esperar que la aplicación y la herramienta funcionen como deben, sino evaluar los comportamientos y efectos de borde que pueden ser objeto de prueba por parte de los potenciales intrusos.

Identificación de las fallas de seguridad informática

	2002 %	**2003 %**	**2004 %**	**2005 %**	**2007 %**	**2008 %**
Material o datos alterados	24,2	22,6	19,3	14	23	20,1
Análisis de registros de auditoría/sistema de archivos/registros *Firewall*	28,8	27	26,0	29	54	33
Sistema de detección de intrusos	9,2	10,2	17,3	17	29,2	21,18
Alertado por un cliente/proveedor	16,3	16,8	10,0	11	27,4	19,70
Alertado por un colega	11,1	12,4	13,7	9	23,9	14,77

Seminarios o conferencias Nacionales e internacionales	3,9	2,9	7,0	8	7,1	4,92
Otro, especifique: revisión manual, pérdida del servicio	6,5	8	6,7	12	7,1	4,43

Comentarios generales:

Los sistemas de detección de intrusos, la identificación de datos alterados y los *firewalls* son las fuentes primarias para la detección de posibles fallas de seguridad en las infraestructuras de computación. Si esto es correcto, el análisis del incidente es la acción seguida requerida para confirmar o no la presencia de un intruso o falla en el sistema. La interacción con colegas y proveedores son 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 Colombia es una tendencia emergente.

Notificación de un incidente de seguridad informática

	2002%	**2003%**	**2004%**	**2005%**	**2007%**	**2008%**
Asesor legal	13,9	9,5	10,6	13	9,7	11,82
Autoridades locales/regionales	5,9	3,8	2,1	7	11,5	5,41
Autoridades nacionales	3	5,7	1,6	9	4,4	5,41
Equipo de atención de incidentes	23,8	32,4	21,8	21	39,8	24,63
Ninguno: No se denuncian	39,6	34,3	50,5	43	47,8	30,04
[ ] Otro	13,9	14,3	13,3	7	-	-

Comentarios generales:

Los datos de este año muestran un ligero incremento de la vinculación de los asesores legales en temas asociados con incidentes de seguridad. Esto puede sugerir una mayor comunicación entre las áreas técnicas y los abogados de las áreas jurídicas, para adelantar un trabajo en equipo más coordinado y formal. De otra parte la cifra de 30% que no denuncia el incidente preocupa en la medida que se hace necesario avanzar en la formación de especialistas en derecho informático, fortalecimiento de la legislación sobre delincuencia informática y formación de especialistas en informática forense como estrategias para enfrentar la amenaza creciente del cibercrimen. Es de resaltar la labor que actualmente adelanta la unidad de delitos informáticos de DIJIN en

la Policía Nacional, así como sus semejantes en el DAS y la Fiscalía General de la Nación.

Si decide no denunciar

	2002 %	2003 %	2004%	2005 %	2007 %	2008 %
Pérdida de valor de accionistas	2,5	7,1	5,6	8	10,7	6,93
Publicación de noticias desfavorables	30	26,3	24	15	31,2	24,27
Responsabilidad legal	13,8	10,1	11,6	14	22,3	11,56
Motivaciones personales	16,3	14,1	17,6	20	22,3	15,60
Vulnerabilidad ante la competencia	17,5	20,2	20,4	16	25	22,54
Otro, especifique: manejo interno de la empresa, desconocimiento	20	22,2	20,8	27	26,8	19,07

Comentarios generales:

La publicación de noticias desfavorables, la vulnerabilidad ante la competencia y algunas veces el desconocimiento sobre el tema y sus procedimientos, son las tendencias más significativas de los resultados de esta sección. Los responsables de la seguridad informática 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 informática articulados con aquellos identificados para los procesos de negocio, debe ser un imperativo que produzca sistemas de gestión de seguridad y de proceso más resistente, resilente y confiable. Es importante anotar, que cada vez más se establecen legislaciones o estándares de aplicación obligatorios como medidas para procurar un proceso continuado de administración de los riesgos de la seguridad de la información, algunos ejemplos la nueva norma de la Superfinanciera de Colombia sobre seguridad informática, lo contemplado en el ISO27002 y 27003, el FISMA (Federal Information Security Management Act) y las directrices del ENISA Europeo.

Herramientas y prácticas de seguridad

No. De pruebas de seguridad realizadas

	2002 %	**2003%**	**2004%**	**2005%**	**2007%**	**2008%**
Una al año	25,7	28,4	29,4	30	31,3	28,02

Entre 2 y 4 al año	29,5	27,5	28,8	30	21,8	29,67
Más de 4 al año	17,1	14,7	11,9	14	10,2	10,99
Ninguna	27,6	29,4	30,0	26	36,7	31,32

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 31% no hace ningún esfuerzo en este sentido. Estas cifras deben llevarnos a meditar en la inseguridad de la información, esa dualidad 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

	2002 %	**2003%**	**2004 %**	**2005 %**	**2007 %**	**2008 %**
Smart Cards	4	1,8	2,4	3	15	11,3
Biométricos (huella digital, iris, etc.)	2,1	1,9	1,6	2	18,4	19,7
Antivirus	0	17,6	16,2	14	86,4	76,4
Contraseñas	21,6	16,2	15,9	13	85	78,3
Cifrado de datos	10,2	7,8	7,7	7	39,5	42,9
Filtro de paquetes	7,4	5,6	6,3	7	34,7	28,1
Firewalls Hardware	8,8	8,5	8,5	8	55,1	49,3
Firewalls Software	8,6	11,1	11,5	12	66	58,1
Firmas digitales/ certificados digitales	3,3	4,4	3,5	5	33,3	27,6
VPN/IPSec	7,2	5,5	5,5	7	44,2	51,2
Proxies	16,3	10,9	11,1	11	49,7	54,2
Sistemas de detección de intrusos	6	5,3	5,9	7	29,9	27,1
Monitoreo 7x24	3,7	2,8	3,5	3	25,2	22,7
Sistemas de prevención de intrusos	-	-	-	-	27,9	20,7

Sistemas de detección de anomalías - ADS	-	-	-	-	3,4	4,93
Firewalls de aplicaciones web - WAF	-	-	-	-	-	22,2
Administración de Logs	-	-	-	-	-	26.6
Ninguna	-	-	-	-	-	0,99
Otro, especifique: *antispyware, antispam, honeypots, inForce,* monitoreos transaccionales	0,7	0,5	0,3	1	4,8	-

Comentarios generales:

Las cifras en 2008 muestran a los antivirus, las contraseñas, los *firewalls* de *software* y *hardware* como los mecanismos de seguridad más utilizados, seguidos por los sistemas VPN y proxies. Dichas tendencias son semejantes con las presentadas por el 2007 CSI/FBI *Computer Crime and Security*, donde se presentan como las tecnologías más sobresalientes: los antivirus, los firewalls, las VPN y los sistemas antispyware. Este mismo informe muestra un marcado interés por las herramientas de cifrado de datos y los firewalls de aplicaciones web que establecen dos tendencias emergentes ante las frecuentes fugas de información y migración de las aplicaciones web al contexto de servicios o *web services*. Adicionalmente anota el informe de Deloitte & Touche, 2007 *Privacy and data protection survey*, que las tecnologías de cifrado de datos, se están incorporando de manera inconsistente, algunas veces para los datos residentes en equipos locales y no para los dispositivos móviles y viceversa, lo que muestra que los ejercicios de clasificación y manejo de información deben entrar en una revisión detallada en el contexto de los procesos de negocio y las necesidades de protección de la misma.

¿Cómo se entera de las fallas de seguridad?

	2002 %	**2003 %**	**2004 %**	**2005 %**	**2007 %**	**2008 %**
Notificaciones de proveedores	23,7	23,8	21,2	23	39,5	33,49
Notificaciones de colegas	24,2	20,3	22,9	19	40,1	36,94

Lectura de artículos en revistas especializadas	26,8	26,4	28,8	24	55,1	49,75
Lectura y análisis de listas de seguridad (BUGTRAQ, SEGURINFO, NTBUGTRAQ, etc.)	16,2	18,5	20,0	26	45,6	43,84
No se tiene este hábito.	9,1	11	7,1	8	22,4	20,19

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 nota 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 1800 participantes desde su fundación en el año 2000.

Políticas de seguridad

Estado actual de las políticas de seguridad

	2002%	**2003%**	**2004%**	**2005%**	**2007%**	**2008%**
No se tienen políticas de seguridad definidas	25	27,5	28,8	23	27,9	22,53
Actualmente se encuentran en desarrollo	48,1	49	46,8	44	43,5	45,05
Política formal, escrita documentada e informada a todo el personal	26,9	23,5	24,4	33	28,6	32,42

Comentarios generales:

El 67,6 % de las empresas en Colombia no cuentan con política de seguridad definidas formalmente o se encuentran en desarrollo. Esta cifra muestra que si bien se ha avanzando en temas de tecnologías de seguridad de la información, las políticas de seguridad aún requieren un esfuerzo adicional conjunto entre el área de negocio y la de tecnología. La seguridad de la información por reacción y como apoyo a las funciones de negocio, es más costosa en el

largo plazo; mientras una función de seguridad articulada con las estrategias de negocio y vinculada a la visión de los clientes, puede generar mucho más valor y asimilar mejor las fallas de seguridad que se presenten.

Principal obstáculo para desarrollar una adecuada seguridad

	2002 %	2003 %	2004%	2005 %	2007 %	2008 %
Inexistencia de política de seguridad	20	22,7	17,0	16	36,1	29,06
Falta de tiempo	17,1	14	23,5	18	32,7	31,52
Falta de formación técnica	12,1	16,3	8,5	7	26,5	26,6
Falta de apoyo directivo	13,6	15,1	18,3	23	34	29,5
Falta de colaboración entre áreas/ departamentos	12,1	14,5	9,8	13	28,6	29,5
Complejidad tecnológica	12,9	6,4	7,8	9	16,3	12,8
Poco entendimiento de la seguridad informática	12,1	11	15,0	14	29,9	28,07
Otro: Asignación presupuestal, falta de recurso humano, cultura de la empresa	-	-	-	-	8,8	4,92

Comentarios generales:

La falta de tiempo, la inexistencia de una política de seguridad de la información, la falta de apoyo directivo y el poco entendimiento de la seguridad informática 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 regular, adaptar y aprender de la inseguridad como la fuente misma de la protección de los negocios de la organización.

Contactos para seguir intrusos

	2002 %	2003 %	2004 %	2005%	2007%	2008%
Si	13,5	11,7	7,4	61	8,2	7,69
No	72,1	66	66,4	30	61,9	64,29
No sabe	14,4	22,3	26,2	9	29,9	28,02

Autoridades que se contactan

Autoridades	2008 %
DAS - ATA	7,14
Dijín	21,43
Fiscalía, Policía Nacional	7,14
HTCIA	7,14
interpol,	7,14
Interpol, Das, Dijín	7,14
ori, minint	7,14
OSRI	7,14
Si	7,14
SIJIN	7,14
Sijín, DAS	7,14
Unidad de delitos Informáticos DAS	7,14

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 estas y sus infractores, bien sea por desconocimiento o por el riesgo de imagen que implica para la organización. Adicionalmente, dada la limitada legislación en temas de delito informático en el país, adelantar un proceso jurídico puede resultar más costoso para la organización que para el posible infractor, dado 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.

En este punto la academia, los gremios, el Gobierno, los proveedores y los usuarios deben organizarse en un frente común para construir estrategias de combate del crimen organizado y en la construcción de modelos de seguridad

resistentes a los embates de la inseguridad de la información. Adicionalmente establecer acuerdos interinstitucionales 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

Estándar o Buena Práctica	2008%
ISO 27001	51,232
Common Criteria	5,91
Cobit 4.1	22,66
Magerit	5,9113
Octave	2,4631
Guías NIST	14,286
Guías ENISA	1,4778
Top SANS	9,8522
OSSTM	7,3892
ISM3	3,9409
Otra	22,66

Norma	2008%
Ninguna	48,11
Sarbanes Oxley	10,37
Superintendencia Financiera	19,81
CRT	12,73
Otra	8,96

Comentarios generales:

Esta es una nueva pregunta que se incluye en esta versión de la encuesta. Los resultados sugieren que en Colombia el ISO 27000, el Cobit 4.1 y las Guías del NIST 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 la norma de la Superfinanciera de Colombia, 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 la Banca, para generar un esfuerzo común en procura de una cultura de seguridad de la información más homogénea y dinámica.

Conclusiones generales

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

1. Las regulaciones nacionales e internacionales llevarán a las organizaciones en Colombia a fortalecer los sistemas de gestión de la seguridad de la información. Actualmente la norma de la Superfinanciera comienza a cambiar el panorama de la seguridad de la información en la Banca y en el país.
2. La industria en Colombia exige más de dos años de experiencia en seguridad informática como requisito para optar por una posición en esta área. De igual forma, se nota que poco a poco el mercado de especialistas en seguridad de la información toma fuerza, pero 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 para 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 las redes y sus componentes, así como la protección de datos de los clientes y un ligero interés en el tema de control de la propiedad intelectual y derechos de autor. Llama la atención la aparición del tema de pólizas de cibercrimen, como un elemento emergente que se empieza a imponer a nivel internacional, como un nuevo control que obliga a las organizaciones a mantener un ejercicio permanente de evaluación de seguridad.
5. Las cifras en 2008 muestran a los antivirus, las contraseñas, los firewalls de *software* y *hardware* 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 los *firewalls* de aplicaciones *web* que establecen 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 legislación en temas de delito informático en el país para adelantar un proceso jurídico puede resultar más costoso para el demandante que para el posible infractor, dado que generalmente la carga de la prueba está a cargo de la parte afectada y los posibles costos derivados de peritaje informático o análisis forense no son coherentes con la economía procesal requerida.
7. Si bien están tomando fuerza las unidades especializadas en delito informático en Colombia, 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 inexistencia de políticas de seguridad 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. ¡Usted decide!
9. Los resultados sugieren que en Colombia el ISO 27000, el Cobit 4.1 y las Guías del NIST son el estándar y las buenas prácticas que están en las áreas de seguridad de la información o en los departamentos de tecnología informática.
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.

Referencias

- *COMPUTER SECURITY INSTITUTE (2007) CSI/FBI Computer Crime and Security Survey 2007.*
- *PRICEWATERHOUSECOOPERS – UK (2008) Information Security Breaches Survey 2008.*
- *PRICEWATERHOUSECOOPERS (2007) 2007 Global State of Information Security Study.*
- *IBM XFORCE (2007) X-Force 2007 Trend Statistics.*
- *DELOITTE & TOUCHE (2007) 2007 Privacy and data protection survey*

Notas

[1]Agradecimientos especiales al Ing. y M.Sc (c) Andrés Almanza por su apoyo y trabajo logístico para contar con la tabulación de los datos de la encuesta. Así mismo, la disposición y oportunidad de la Ing. Liliana Baquero, para adelantar con oportunidad y efectividad la encuesta nacional de seguridad informática.