

VII Encuesta Nacional de Seguridad Informática

Jeimy J. Cano, Ph.D, CFE

Panorama colombiano y las tendencias en 2007.

Este año la participación en la VII Encuesta Nacional de Seguridad Informática ascendió a 223 personas (en comparación con las 182 del 2005), con lo cual los resultados que se presentan en esta edición cuentan con mayor población de los diferentes sectores productivos sobre el tema de seguridad informática en el país.

Es importante anotar que en 2006 el número de personas participantes no fue estadísticamente significativo y por lo tanto, no se presentaron los resultados de la encuesta.

El análisis presentado a continuación se desarrolló basado en una muestra aleatoria, la cual respondió a los interrogantes 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, el cual pretende 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 *2006 Australian Computer Crime and Security Survey*, el *2006 CSI/FBI Computer Crime and Security Survey*, el *Information Security Breaches Survey 2006* y el *IBM X-Force 2006 Trend Statistics* se procederá a analizar los resultados.

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 adecuada seguridad; los contactos nacionales e internacionales para seguir posibles intrusos.

Consideraciones muestrales

Considerando una población limitada (alrededor de 1400 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 178 participantes. Al contar con 223 participantes en la muestra, los resultados presentados son estadísticamente representativos.

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

Demografía

Sectores participantes:

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

Comentarios generales:

Los resultados muestran una participación activa del sector educativo, el Gobierno, la banca y la industria informática. 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. Así mismo, es importante anotar la nueva regulación en

materia de seguridad informática que formalizará durante este año la Superintendencia Financiera, entidad que acelerará los cambios previstos para la banca y el sector financiero en general. Si esto ocurre, será un catalizador de una dinámica necesaria para impulsar otros sectores donde estos temas aún no tienen el alcance ni el nivel organizacional y de negocio.

Número de empleados de la organización

	AÑO 2002 %	AÑO 2003 %		AÑO 2004 %	AÑO 2005 %	AÑO 2007 %
1 a 100	31,4	19	1 a 50	27,9	28	27,3
101 a 250	17,6	13,3	51 a 100	11,6	19	12,9
251 a 500	10,8	18,1	101 a 200	13,0	11	7,7
501 a 1000	11,8	16,2	201 a 300	3,3	5	7,2
1001 a 2500	11,8	16,2	301 a 500	11,2	12	10,8
2501 a 5000	8,8	11,4	501 a 1000	11,6	13	9,3
Más de 5000	7,8	5,7	Más de 1000	21,4	13	24,7

Comentarios generales:

Es interesante observar que la pequeña mediana y grande industria participaron con porcentajes similares en la encuesta. Se mantiene la tendencia de años anteriores donde las pequeñas y medianas ven en la seguridad un factor diferenciador y generador

de confianza. Por su parte, la gran empresa muestra un renovado interés en participar y avanzar en los temas de seguridad de la información, pues las regulaciones nacionales e internacionales establecen referentes que no pueden ser ignorados en materia de seguridad informática.

Número de personas dedicadas a seguridad informática

	AÑO 2002 %	AÑO 2003 %	Diferencia porcentual
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 %
Ninguna	26,8	26	28,6
1 a 5	58,2	58	54,9
6 a 10	10,9	5	10,9
11 a 15	0,9	5	0,5
Más de 15	3,2	6	5,2

Comentarios generales:

Los resultados de este año permanecen constantes y con un ligero

incremento porcentual en el caso de no tener a ninguna persona de tiempo completo en el tema de seguridad

informática. Sin embargo, podemos observar un importante aumento en la porción de 6 a 10 personas de tiempo completo, hecho que sugiere un renovado interés de la organización para formalizar el área de seguridad de la información. Se muestra

una aparente contradicción, pero se explica con el hecho de que las grandes empresas y la banca tienden a organizarse para cumplir con las regulaciones que sobre el tema se vienen presentando en el contexto nacional e internacional.

Dependencia organizacional del área de seguridad informática

	2002 %	2003 %	2004 %	2005 %	2007 %
Auditoría interna	5	3,9	6,1	7	4,8
Director de Seguridad Informática	11,9	14,7	10,2	18	20,5
Director Departamento de Sistemas/Tecnología	60,4	52,9	53,8	39	44,6
Gerente Ejecutivo	4	2	1,5	4	0,6
Gerente de Finanzas	0	1	1	0	0
No se tiene especificado formalmente	11,9	22,5	18,3	21	17,5
Otro, especifique: Riego operativo, Vicepresidencia de Operaciones, Jefe de Telemática, etc.	6,9	2,9	9,1	11	12

Comentarios generales:

A pesar de un importante incremento de directores de seguridad informática, la tendencia de que el área de seguridad de la información esté en el Departamento de Sistemas o de Tecnología, se mantiene. Así mismo, se observa que las organizaciones

van adquiriendo conciencia de la necesidad de contar con el área de seguridad informática. No obstante, esta área continúa teniendo un matiz eminentemente tecnológico y operacional, lo que limita su participación en decisiones de negocio o estratégicas de las organizaciones.

Años de experiencia requeridos para trabajar en seguridad informática

	2007 %
Ninguna	6,6
Menos de un año de experiencia	10,7
Uno a dos años	38,5
Más de dos años	44,3

Comentarios generales:

Se introduce este año esta pregunta relevante para el sector de la seguridad informática. El mercado laboral exige en promedio de más de dos años de experiencia en seguridad de la información; una cifra que exige de los profesionales que quieren ingresar a este mercado una formación técnico-práctica y certificaciones tanto de producto como generales (las cuales

serán analizadas más adelante), que permiten validar la misma. En ese sentido, la academia está en mora de fortalecer líneas de investigación en esta área para responder a esta creciente demanda, no sólo para generar fuerza de trabajo ajustada a los perfiles empresariales, sino investigadores que continúen desarrollando nuevas aplicaciones y conceptos aplicables a la realidad colombiana.

Certificaciones en seguridad informática

	2007 %
Ninguna	60,3
CISSP	20,7
CISA	14,9
CISM	9,9
CFE	0,8
CIFI	5,8
CIA	10,7
Otras: Especializaciones en Auditoría de Sistemas, Diplomados en Seguridad Informática, Auditor Líder BS7799, Certified Ethical Hacking, CCNA, CCSP, GSEC, MCSE, etc.	18,2

Comentarios generales:

Al igual que la anterior, esta pregunta es nueva en la versión de 2007. Los resultados muestran que a pesar de que existen múltiples certificaciones en el tema de seguridad de la información, auditoría de sistemas, fraude, informática forense y auditoría interna, las personas que trabajan en las áreas de seguridad no cuentan con alguna de ellas. Es importante anotar que las certificaciones como iniciativa de la

industria por generar un cuerpo de conocimiento requerido para los profesionales de la seguridad informática, son diferenciadores importantes a la hora de ganar negocios o licitaciones y alcanzar alguna posición laboral. Sin embargo, es necesario fortalecer la creación de programas académicos formales que busquen consolidar iniciativas en estos temas, con miras a la formación de investigadores y profesionales de nivel internacional.

Importancia de contar con certificaciones en seguridad informática

	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

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 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. Si bien esta tendencia

es clara en la encuesta, la experiencia comprobada y los resultados de alta calidad en proyectos de seguridad de la información son también valorados para adelantar iniciativas en los temas de seguridad informática en las organizaciones colombianas. Un balance entre certificaciones, práctica y formación académica establecen factores diferenciadores y atractivos para el profesional en seguridad de la información y las organizaciones.

Cargos que respondieron la encuesta

	2002 %	2003 %	2004 %	2005 %	2007 %
Presidente/Gerente General/Director Ejecutivo	8,5	6,7	9,8	5	7,2
Director/Vicepresidente	16	8,6	5,2	6	3,6
Director/Jefe de Seguridad Informática	11,3	15,2	8,2	14	10,2
Profesional del Departamento de Seguridad Informática	11,3	3,8	8,8	11	12,7
Profesional de Departamento de Sistemas/Tecnología	35,8	46,7	44,8	36	36,1
Auditor Interno	2,8	2,9	4,1	4	1,2
Otro, especifique: Director de IT y Seguridad, Administrador de la red, Director de Investigación y Desarrollo, Investigador Criminalístico, Gerente de proyectos, Consultor de seguridad.	14,2	16,2	19,1	24	27,1

Comentarios generales:

Estos resultados marcan la tendencia generalizada de una seguridad informática dentro de las áreas de tecnología de información, como un fenómeno técnico y operacional. No obstante, se mantiene la participación de la alta gerencia, lo que sugiere vigente el interés en los temas de seguridad, los cuales no son ajenos a este

nivel. Contrario a lo que se piensa en las áreas de informática, la alta gerencia está ávida de conocer el estado de la seguridad, pero la incompatibilidad de lenguajes, los canales de comunicación establecidos y los diversos intereses de negocio dificultan la interacción entre el encargado de la seguridad y las áreas estratégicas de la organización.

Presupuesto

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

	2002 %	2003 %	2004 %	2005 %	2007 %
Protección de la red	19,3	22,7	20,6	19	74,1
Proteger los datos críticos de la organización	19,8	19,5	18,8	18	62
Proteger la propiedad intelectual	8,9	3,7	6,1	6	21,1
Proteger el almacenamiento de datos de clientes	12,8	13,7	11,7	12	47,6
Concientización/formación del usuario final	7,8	7,4	9,2	8	28,3
Comercio/negocios electrónicos	4,7	4	6,5	5	10,8
Desarrollo y afinamiento de seguridad de las aplicaciones	9,4	10,3	8,1	11	27,1
Asesores de seguridad informática	5,5	5,8	6,3	7	20,5
Contratación de personal más calificado	1,8	1,8	2,0	3	13,9
Evaluaciones de seguridad internas y externas	9,9	9,8	9,6	4	25,9
Monitoreo de Seguridad Informática 7x24	-	-	-	-	25,3
Otro, especifique: Ninguno, Capacitación, auditoría, certificaciones de seguridad, continuidad del negocio	0,3	1,3	1,1	0	27,1

Comentarios generales:

Los resultados este año reafirman la tendencia de la inversión en seguridad, concentrada en zona perimetral, en las redes y sus componentes, como factor crítico dentro del modelo corpo-

rativo de seguridad de la información. En esa misma línea, la protección de los datos críticos de la organización y de los clientes, como referente natural de la función de seguridad en las organizaciones. Estos datos son

coherentes con los resultados expuestos por el *Information Security Breaches Survey 2006* adelantado en el Reino Unido en conjunto con PriceWaterhouseCoopers, donde se

indican como motivadores claves de la seguridad proteger la información del consumidor, mantener la integridad de los datos y la protección de la reputación de la organización.

Presupuesto previsto para seguridad informática 2006

	2003 %	2004 %	2005 %	2007 %
Menos de USD\$50.000	64,3	58,1	50	67,9
Entre USD\$50.001 y USD\$70.000	12,2	15,2	21	12,7
Entre USD\$70.001 y USD\$90.000	3,1	5,7	6	7,3
Entre USD\$90.001 y USD\$110.000	3,1	6,7	8	1,8
Entre USD\$110.001 y USD\$130.000	4,1	3,8	3	3
Más de USD\$130.000	13,3	10,5	12	7,3

Comentarios generales:

En 2006 la inversión en seguridad informática sufrió un retroceso importante en la pequeña y mediana industria. Algunas de las razones para este comportamiento se relacionan con los altos costos de la consultoría, el hardware y el software en temas de seguridad de la información, entre otros aspectos. Es probable que durante los próximos años, con el advenimiento de regulaciones nacionales e internacionales estas cifras cambien.

La encuesta 2006 *Australian Computer Crime and Security Survey*, muestra que las empresas australianas disminuyeron su inversión en seguridad informática a un incremento del 5% del presupuesto total de las tecnologías de información, mientras en el año anterior se observaban incrementos entre el 7% y el 12%. Las tensiones de los mercados internacionales y las caídas de las principales bolsas del mundo afectaron las utilidades de las empresas y por tanto sus presupuestos para los temas de tecnología y seguridad.

Presupuesto previsto para seguridad informática 2007

	2007 %
Menos de USD\$50.000	61,8
Entre USD\$50.001 y USD\$70.000	13,3
Entre USD\$70.001 y USD\$90.000	4,8
Entre USD\$90.001 y USD\$110.000	6,1
Entre USD\$110.001 y USD\$130.000	1,8
Más de USD\$130.000	12,1

Comentarios generales:

Las proyecciones de las organizaciones en los temas de inversión en seguridad sugieren incrementos moderados. A pesar de ello, en las grandes organizaciones generalmente representadas por el sector bancario y de telecomunicaciones, se notan importantes inversiones en materia de seguridad, en su mayoría motivados por aspectos tales como el cumplimiento de la normatividad y las pólizas de seguro, los cuales se convierten en disparadores de la dinámica de la función de seguridad.

Estas tendencias se confirman en el informe *2006 CSI/FBI Computer Crime and Security Survey*, en el que se destaca que el 80% de las organizaciones se ha sometido a auditorías de seguridad informática y que las exigencias de cumplimiento de regulaciones impactan en forma sustancial la función de seguridad informática demandando de esta mayores niveles de efectividad y eficiencia frente al nivel de inversión que se hace en la misma.

Fallas de seguridad

Tipos de fallas de seguridad

	2002 %	2003 %	2004 %	2005 %	2007 %
Ninguno	5,4	8,7	6,6	9	5,3
Manipulación de aplicaciones de software	4,5	4,3	5,8	8	24,8
Accesos no autorizados al web	14,8	10,6	9,4	10	35,4
Fraude	4	3,9	1,8	5	13,3
Virus	33,6	33,3	34,9	29	62,8
Robo de datos	3,6	3,9	2,6	2	10,6
Caballos de Troya	4,9	4,8	10,0	11	29,2
Monitoreo no autorizado del tráfico	4,9	7,7	5,8	8	7,1
Negación del servicio	6,3	7,2	7,6	7	21,2
Pérdida de integridad	6,7	3,9	2,9	3	12,4
Pérdida de información	9,4	10,1	10,5	7	24,8
Phising	-	-	-	-	17,7
Pharming	-	-	-	-	3,5
Otros, especifique: pérdida de laptops, acceso no autorizado a equipos, fuga de información, spyware.	1,8	1,4	2,1	1	6,2

Comentarios generales:

Una vez más, los virus, el código malicioso o *malware* son la causa más frecuente de las fallas de seguridad en las organizaciones colombianas, seguido por los accesos no autorizados vía web y los Caballos de Troya. Estas tres tendencias la confirman los estudios efectuados por el IBM *Xforce 2006 trend statistics*, donde se establece que:

- Aproximadamente el 50% de los sitios web contienen códigos maliciosos diseñados para infectar navegadores web y ofuscar sus ataques. Aproximadamente el 30% de ellos cifran sus conexiones y descargas.

- El 88.4% de todas la vulnerabilidades del 2006 pueden ser materializadas de manera remota.

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 contemplan, así como los procedimientos de instalación y configuración de las herramientas de seguridad respectivamente. Luchar contra la inseguridad de la información no es solo 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 %
Material o datos alterados	24,2	22,6	19,3	14	23
Análisis de registros de auditoría/sistema de archivos/registros Firewall	28,8	27	26,0	29	54
Sistema de detección de intrusos	9,2	10,2	17,3	17	29,2
Alertado por un cliente/proveedor	16,3	16,8	10,0	11	27,4
Alertado por un colega	11,1	12,4	13,7	9	23,9
Seminarios o conferencias Nacionales e internacionales	3,9	2,9	7,0	8	7,1
Otro, especifique: No me di cuenta, revisión manual, pérdida del servicio	6,5	8	6,7	12	7,1

Comentarios generales:

Los sistemas de detección de intrusos 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 sobre fallas se perfila como una marcada tendencia en el entorno colombiano.

Notificación de un incidente de seguridad informática

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

Comentarios generales:

Los datos de este año destacan casi un 40% de casos notificados y apoyados por equipos de atención de incidentes, resultado que muestra el interés de la organización para ser preactiva, frente a una falla de seguridad de la información, en procura del debido cuidado de los activos de la organización. Dicha cifra contrasta con un 48% que no denuncia el incidente, quienes muchas veces

no lo hacen por falta de formación en temas de derecho informático, en legislación sobre delincuencia informática y limitados cuerpos gubernamentales o unidades especializadas en estos temas. Es de resaltar la labor que en la actualidad adelanta la unidad de delitos informáticos de la 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 %
Pérdida de valor de accionistas	2,5	7,1	5,6	8	10,7
Publicación de noticias desfavorables	30	26,3	24	15	31,2
Responsabilidad legal	13,8	10,1	11,6	14	22,3
Motivaciones personales	16,3	14,1	17,6	20	22,3
Vulnerabilidad ante la competencia	17,5	20,2	20,4	16	25
Otro, especifique: pérdida de información, manejo interno de la empresa, desconocimiento	20	22,2	20,8	27	26,8

Comentarios generales:

La publicación de noticias desfavorables, la vulnerabilidad ante la competencia y la responsabilidad legal 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 ese 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 resistentes y confiables. Es importante anotar, que con mayor frecuencia se establecen regulaciones de obligatorio cumplimiento, como medidas para procurar un proceso continuado de administración de los riesgos de la seguridad de la información, algunos ejemplos son la nueva norma de la Superfinanciera de Colombia sobre riesgo operativo, la próxima norma de seguridad de la información de la misma entidad, lo contemplado en el ISO27001 y el FISMA (Federal Information Security Management Act).

Herramientas y prácticas de seguridad

Número de pruebas de seguridad realizadas

	2002 %	2003 %	2004 %	2005 %	2007 %
Una al año	25,7	28,4	29,4	30	31,3
Entre 2 y 4 al año	29,5	27,5	28,8	30	21,8
Más de 4 al año	17,1	14,7	11,9	14	10,2
Ninguna	27,6	29,4	30,0	26	36,7

Comentarios generales:

Los resultados de esta sección son contrastantes. Por un lado, un grueso de la población adelanta por lo menos una prueba al año, mientras el 37% no hace ningún esfuerzo en tal 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 hasta dónde pueden llegar. Por tanto, no hacerlo es arriesgarse a ser parte formal de las estadísticas de aquellos para quienes la seguridad es sólo un referente tecnológico.

Mecanismos de Seguridad

	2002 %	2003 %	2004 %	2005 %	2007 %
Smart Cards	4	1,8	2,4	3	15
Biométricos (huella digital, iris, etc.)	2,1	1,9	1,6	2	18,4
Antivirus	0	17,6	16,2	14	86,4
Contraseñas	21,6	16,2	15,9	13	85
Encriptación de datos	10,2	7,8	7,7	7	39,5
Filtro de paquetes	7,4	5,6	6,3	7	34,7
Firewalls Hardware	8,8	8,5	8,5	8	55,1
Firewalls Software	8,6	11,1	11,5	12	66
Firmas digitales/certificados digitales	3,3	4,4	3,5	5	33,3
VPN/IPSec	7,2	5,5	5,5	7	44,2
Proxies	16,3	10,9	11,1	11	49,7
Sistemas de detección de intrusos	6	5,3	5,9	7	29,9
Monitoreo 7x24	3,7	2,8	3,5	3	25,2
Sistemas de prevención de intrusos	-	-	-	-	27,9
Sistemas de detección de anomalías - ADS	-	-	-	-	3,4
Otro, especifique: antispymware, antispam, honeypots, inForce, monitoreos transaccionales	0,7	0,5	0,3	1	4,8

Comentarios generales:

Las cifras en 2007 muestran los antivirus, las contraseñas, los firewalls de hardware y software como los mecanismos de seguridad más utilizados, seguidos por los sistemas de VPN y proxies. Dichas tendencias son semejantes con las presentadas por el *2006 CSI/FBI Computer Crime and Security*, en donde se presentan como las tecnologías más sobresalientes: los

firewalls, los antivirus y los sistemas de detección de intrusos. Este mismo informe muestra un marcado interés por las herramientas de computación forense, no registrado en los resultados de la encuesta en Colombia. Todavía en el país la evidencia digital está abriéndose camino en la administración de justicia y la buena práctica de la seguridad de la información debe ir fortaleciéndola.

¿Cómo se entera de las fallas de seguridad?

	2002 %	2003 %	2004 %	2005 %	2007 %
Notificaciones de proveedores	23,7	23,8	21,2	23	39,5
Notificaciones de colegas	24,2	20,3	22,9	19	40,1
Lectura de artículos en revistas especializadas	26,8	26,4	28,8	24	55,1
Lectura y análisis de listas de seguridad (BUGTRAQ, SEGURINFO, NTBUGTRAQ, etc.)	16,2	18,5	20,0	26	45,6
No se tiene este hábito.	9,1	11	7,1	8	22,4

Comentarios generales:

Los números de esta sección muestran un cambio importante en los hábitos de los profesionales de la seguridad de la información.

La lectura de artículos en revistas especializadas y la lectura y análisis de las listas de seguridad son las fuentes de información más frecuentes en el desarrollo de su

trabajo. Si bien sabemos que la di-námica 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 en torno a la comprensión y

revisión de las fallas de seguridad y su impacto en la organización. SEGURINFO, continúa creciendo, en la actualidad cuenta con 1500 participantes, desde su fundación en el año 2000.

Políticas de seguridad

Estado actual de las políticas de seguridad

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

Comentarios generales:

El 71,4% de las empresas en Colombia no cuentan con una política de seguridad definida de manera formal 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 sobre el tema siguen relegadas y como un asunto que debe desarrollar el área de tecnología. Esta divergencia entre lo tecnológico y lo estratégico muestra cómo el

tema de seguridad no hace parte del negocio de las organizaciones y sólo es considerado crítico cuando un evento infortunado ocurre. 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

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

Comentarios generales:

La inexistencia de una política de seguridad de la información, la falta de tiempo 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 y de la poca creatividad de los profesionales de la seguridad

para vender la distinción de la seguridad y el día a día de la operación de los mecanismos de seguridad. 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 %
Sí, especifique cuáles: DAS, Fiscalía, SUJIN, FBI, Inconcrédito, organismo interno de la empresa	13,5	11,7	7,4	61	8,2
No	72,1	66	66,4	30	61,9
No sabe	14,4	22,3	26,2	9	29,9

Comentarios generales:

Si 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 conductas y sus infractores. Bien sea por desconocimiento o por el riesgo de imagen que implica para la organización. En forma coherente con esta cifra se advierte en una sección anterior, la poca presencia de herramientas forenses que permitan adelantar investigacio-

nes formales sobre los casos que se presentan. Esta situación fortalece la posición del intruso ante un proceso judicial, toda vez que cualquier duda se resuelve a favor del implicado.

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 contra el crimen organizado y en la construcción de modelos de seguridad resistentes a los embates de la inseguridad de la información.



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, no solo para cumplir con lo establecido en la norma ISO 27001, sino en el diseño de sistemas más resistentes y confiables para los usuarios.

2. El mercado de los profesionales de seguridad de la información deman-

da una formación que conjugue la práctica y la experiencia verificables (generalmente asociadas con aspectos tecnológicos y de producto); la formación académica (en programas de educación formal como especializaciones o maestrías); y, las certificaciones generales como factores claves y atractivos para los empleadores.

3. La inversión en seguridad de la información se encuentra concentrada en el perímetro de las organizaciones: redes y sistemas de comunicaciones, mientras los aspectos relacionados con la clasificación de la información y los dispositivos de almacenamiento



móviles aún no son prioridad dentro de las organizaciones.

4. Mientras que las VPN, los proxies y firewalls son elementos fundamentales de los mecanismos de seguridad en las organizaciones colombianas, las herramientas forenses aún no encuentran su lugar ni su justificación para incorporarse al discurso de la seguridad informática en Colombia.

5. Si bien están tomando fuerza las unidades especializadas en delito informático en Colombia, es necesario desarrollar esfuerzos conjuntos entre la academia, el gobierno, las organizaciones y la industria, para mostrarles a los intrusos que estamos preparados para enfrentarlos.

6. 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!

7. Es hora de empezar a medir cuánto nos cuestan los incidentes de seguridad de la información para avanzar en la construcción del indicador de retorno de la inversión, como una manera de saber qué se debe fortalecer, qué es necesario desaprender y cuáles compromisos se deben asumir en el combate de la inseguridad de la información.

Referencias

[1] AUSCERT (2006) 2006 Australian Computer Crime and Security Survey. Disponible en: <http://www.auscert.org.au/images/ACCSS2006.pdf>. (Consultado: 6/05/2007)

[2] COMPUTER SECURITY INSTITUTE (2006) CSI/FBI Computer Crime and Security Survey. Disponible en: <http://www.gocsi.com/>. (Consultado: 6/05/2007)

[3] PRICEWATERHOUSECOOPERS – UK- DTI (2006) Information Security Breaches Survey 2006. Disponible en: http://www.pwc.com/uk/eng/ins-sol/publ/pwc_dti-fullsurveyresults06.pdf. (Consultado: 6/05/2007)

[4] IBM XFORCE (2006) X-Force 2006 Trend Statistics. Disponible en: http://www.iss.net/x-force_report_images/index.html. (Consultado: 6/05/2007)

Jeimy J. Cano, Ph.D, CFE. Miembro investigador del Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática (GECTI), Facultad de Derecho, Universidad de los Andes. Colombia. Miembro Investigador de ALFA-REDI (Red Latinoamericana de Especialistas en Derecho Informático). 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 en Computer Forensic Analysis (CFA) del World Institute for Security Enhancement, USA. Profesional certificado como Certified Fraud Examiner (CFE) por la Association of Certified Fraud Examiners. Coordinador Lista de Seguridad – SEGURINFO (ACIS).