## Seguridad Informática en Argentina – Informe 2011

María Patricia Prandini, MAS, Especialista en Seguridad Informática (UBA), CISA, CRISC
Marcia Maggiore, Especialista en Seguridad Informática (UBA), CISA, CRISC

### Introducción

Se le atribuye a Bill Hewlett (1930-2001), cofundador de Hewlett-Packard, la frase "No se puede gestionar lo que no se puede medir"[1]. El campo de la seguridad informática no escapa a esta afirmación. En efecto, un proceso efectivo de toma de decisiones en una materia tan crítica como esta requiere necesariamente mediciones válidas sobre lo que está ocurriendo.

Sin embargo, por diversos motivos entre los que se encuentran el hecho de tratarse de un área en constante evolución, la reticencia de las organizaciones para compartir datos sobre los incidentes que las han afectado y la falta de métricas estandarizadas, resulta hoy dificultoso contar con información precisa y actualizada en este campo.

Con esta certeza, por segundo año consecutivo el Capítulo Argentino de ISACA (Information System Audit and Control Association–www.adacsi.org.ar) y la Asociación Argentina de Usuarios de la Informática y las Comunicaciones (USUARIA–www.usuaria.org.ar) se sumaron durante el año 2011 a los esfuerzos de la Asociación Colombiana de Ingenieros de Sistemas (ACIS–www.acis.org.co) y de otras organizaciones de Latinoamérica para colectar información relativa a diversos aspectos de la seguridad de la información en la Región.

La información correspondiente a Argentina fue recopilada tomando como base 61 respuestas válidas, superándose en un 50% la cantidad recibida el año anterior. Si bien esta muestra sigue siendo relativamente pequeña se considera valiosa, toda vez que fue enfocada exclusivamente a personal especializado, directamente ligado a la temática a analizar. Por otra parte, siendo este el segundo año en que se realiza, permitirá fijar tendencias en su comparación con el anterior. Asimismo, debe considerarse que no existe en la región otra iniciativa similar de esta naturaleza y extensión. En tal sentido, queremos agradecer a quienes nuevamente completaron la encuesta y a los que se sumaron este año, con la certeza de que los datos provistos contribuirán a profundizar el conocimiento de la seguridad de la información en la región y en nuestro país.

El presente informe resume mediante gráficos los aspectos más relevantes de la encuesta realizada, la cual estuvo conformada por 31 preguntas de tipo "multiple choice" y formula una serie de conclusiones respecto al estado de la seguridad en nuestro país, en función de las respuestas recibidas.

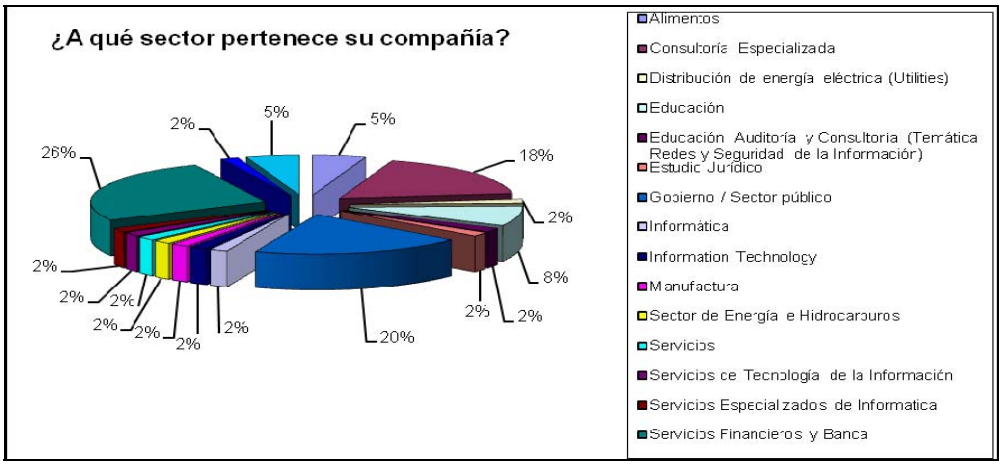
### Análisis de datos

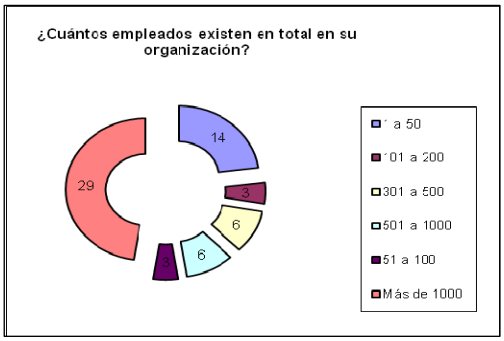
A continuación se presentan los resultados más relevantes de la encuesta mediante gráficos comentados. En los casos aplicables, los datos recopilados se vinculan con los registrados el año pasado.

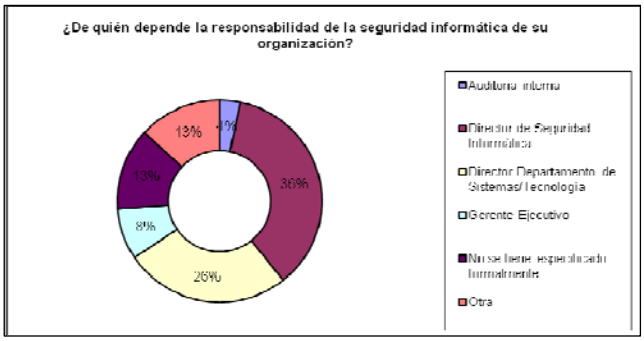
[1] Traducción libre de la frase original en inglés "You cannot manage what you cannot measure"

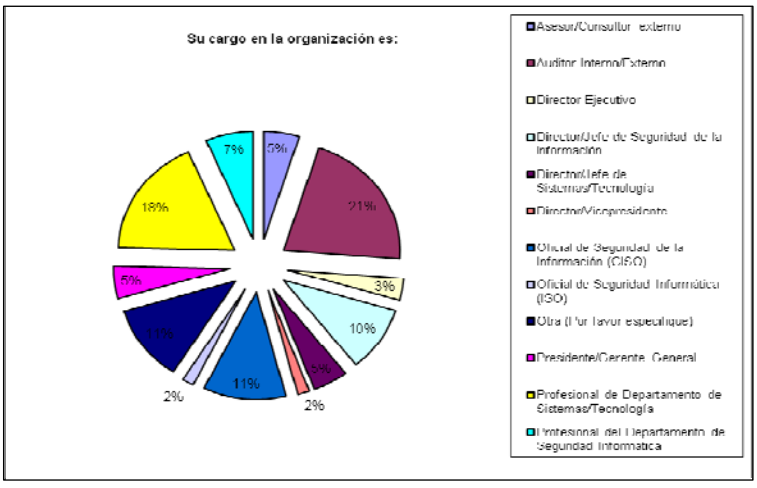
## *1. Perfil de los encuestados*

Esta sección de la encuesta incluye cuatro preguntas vinculadas al sector en que se desempeña el encuestado, la cantidad de empleados que tiene su organización, el cargo que ocupa y el área sobre la que descansan las responsabilidades vinculadas a la Seguridad de la Información.



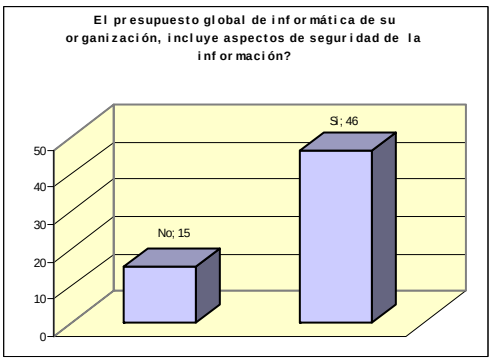

<u>Comentarios generales:</u>

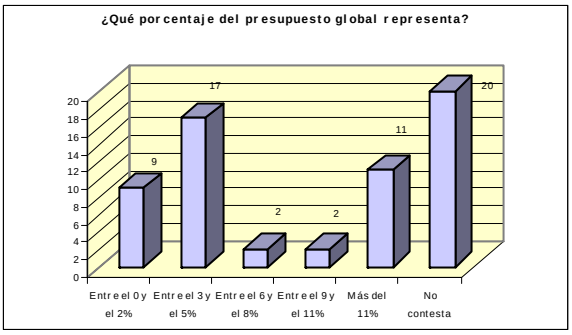
Se observa que la mayoría de las respuestas provienen de profesionales que trabajan en empresas grandes, con plantas de personal que superan el millar de empleados. Si bien este año presenta una distribución levemente más equilibrada, esta característica coincide con los resultados de la encuesta 2010. De los sectores representados, un 25% pertenece

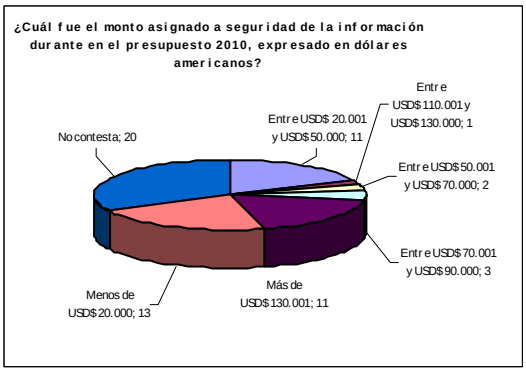
al Sector Financiero seguido del Sector Público y el de Consultoría Especializada. A los sectores ya mencionados, se agregan con porcentajes menores respuestas de los sectores de la Educación, Servicios, Alimentos y Telecomunicaciones, entre otros. En cuanto a los cargos que ocupan los participantes, llama la atención que un 21% son auditores externos/internos, seguidos de personal del área de tecnología y en tercer lugar, del sector de seguridad informática. Un posible motivo para la cantidad de auditores es el hecho de que la distribución de la encuesta se realizó a través del Capítulo local de ISACA, muchos de cuyos socios realizan tareas vinculadas a la auditoría de sistemas. En la encuesta del año pasado, un tercio de quienes respondieron provenía del área de Seguridad Informática, seguidos del grupo de auditores de Tecnología. Respecto a las responsabilidades sobre la seguridad de la información, y mejorando el escenario del año anterior, más de un tercio indica que descansa sobre un área específica mientras que un 26% muestra que depende del área de Tecnología. Sin embargo, el porcentaje de respuestas que señala que las responsabilidades no se encuentran especificadas formalmente es de un 13%, 5 puntos por encima del registrado el año anterior, cuando hubiera sido esperable que la cantidad de respuestas para esta opción hubiera disminuido.

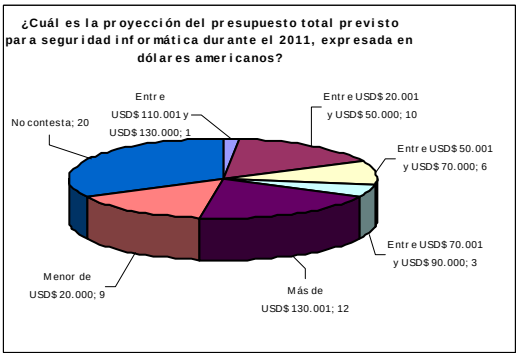
## *2. Presupuesto asignado a la Seguridad Informática*

Esta sección incluye una serie de preguntas relativas a la inclusión en el presupuesto global de la organización de ítems vinculados a la seguridad de la información, al porcentaje que representa, el monto asignado y la proyección para el año 2011.



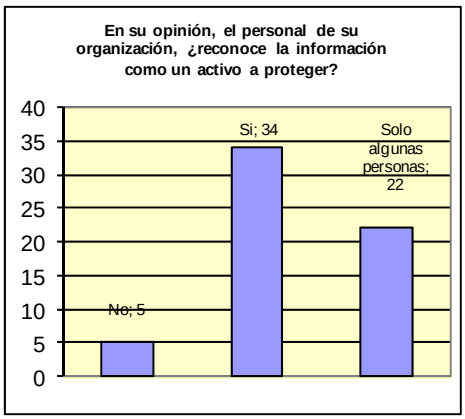

<u>Comentarios generales:</u>

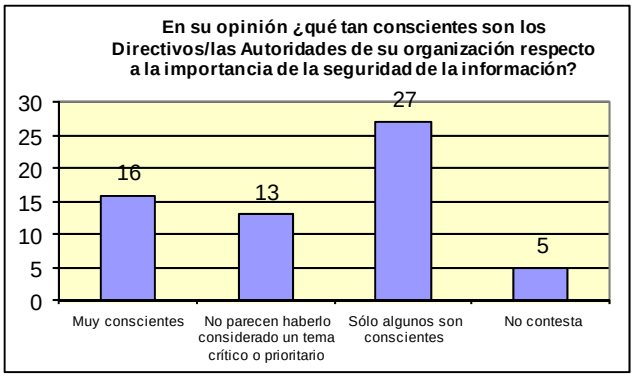
Contrariamente a lo esperado, este año mostró una disminución en el porcentaje de respuestas señalando que el presupuesto asignado al área de Tecnología contaba con partidas específicas para Seguridad. En este caso, sólo un 75% contra el 88% del año pasado, respondió en forma positiva. Sin embargo, al indagar sobre el porcentaje del

presupuesto global asignado al área, un porcentaje mayor se concentró en valores del 3 al 5%, mientras que el año pasado el mayor índice se registró en la opción inferior al 2%. Con relación a la pregunta sobre el monto asignado a la Seguridad, se observa que un tercio no respondió la pregunta, seguramente por desonocer tal asignación. Entre quienes indicaron un monto, nuevamente como el año pasado, las respuestas se mostraron polarizadas. Mientras casi un 20% indicó que contaba con una asignación superior a US$130.000, en el otro extremo, otro tanto señaló contar con menos de US$20.000 dólares. En cuanto a la proyección para el año 2011, y en forma similar a lo ocurrido en la encuesta 2010, se repìtió prácticamente la proporción mostrada en la pregunta anterior. Tal como se señaló el año pasado, estos niveles parecen escasos, a la luz de que, como se vio en secciones anteriores, dentro de los sectores más significativos se encontraban el bancario y el gubernamental, ambos usuarios intensivos de las Tecnologías de la Información, sobre los que basan una parte importante de sus servicios. Por otro lado, resulta desalentador que nuevamente no se prevean mejorías en cuanto a los presupuestos asignados al área de seguridad de la información para el año siguiente, considerando las mayores exigencias regulatorias en la materia y el nivel estratégico de la seguridad de la información para la prestación de los servicios.

### *3. Nivel de Concientización*

En esta sección se presentan las respuestas a dos preguntas vinculadas al reconocimiento del valor de la información como un activo de la organización, desde la perspectiva del personal de la organización y de la de sus directivos y autoridades.



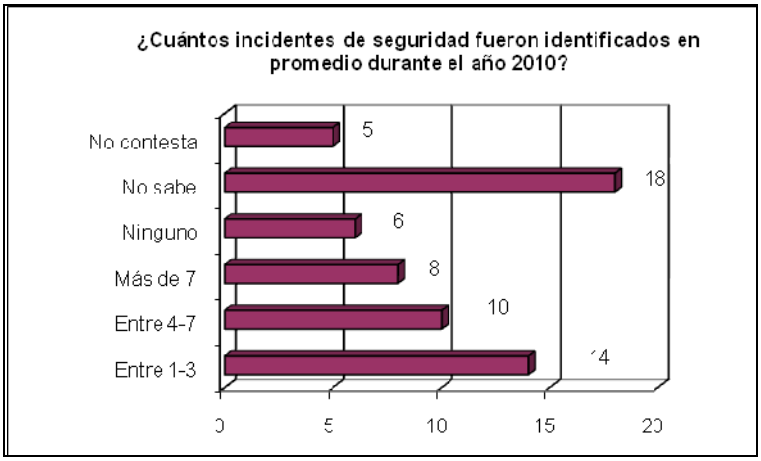



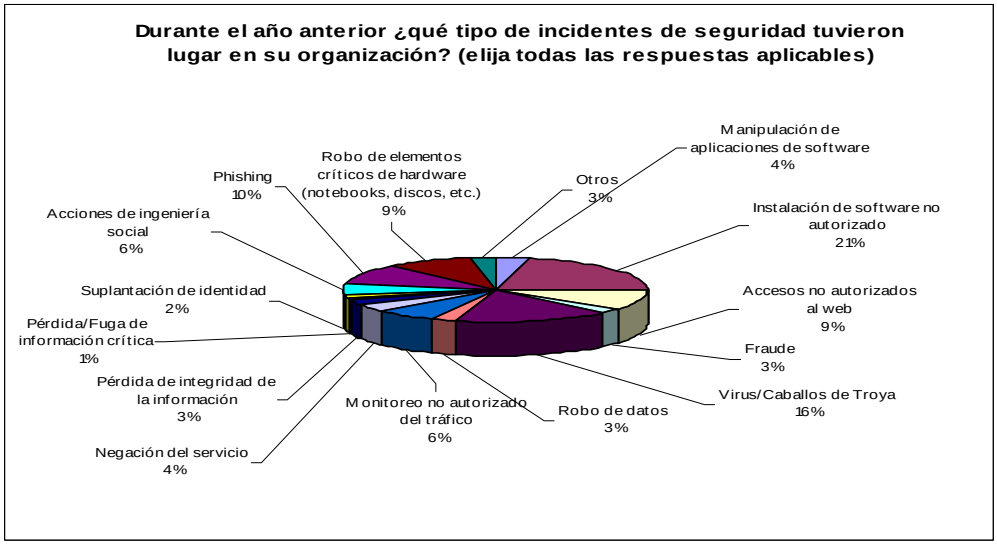

Comentarios generales:

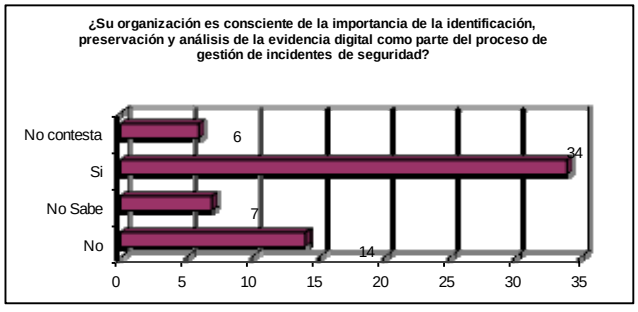
En el caso del primer cuadro, el escenario mejora respecto al año anterior, toda vez que más del 50% indica que el personal es consciente del valor de la información, contra un 21% del año pasado. Sin embargo, esta tendencia se invierte en la segunda opción de respuesta, porque para este año el 33% responde que sólo algunas personas son conscientes, mientras que el año pasado registró un 67%. En cuanto al nivel directivo, un 25% señala que son conscientes y casi un 50% indica que sólo algunos son conscientes. Las respuestas a esta pregunta, que no se formuló en estos términos el año anterior, muestran un escenario desalentador, debido a que un alto porcentaje del personal directivo parece no darle suficiente importancia al tema.

## *4. Gestión de Incidentes de Seguridad*

En esta sección se incluyen preguntas de la encuesta vinculadas a la cantidad y tipo de falla de seguridad y a la evidencia digital.



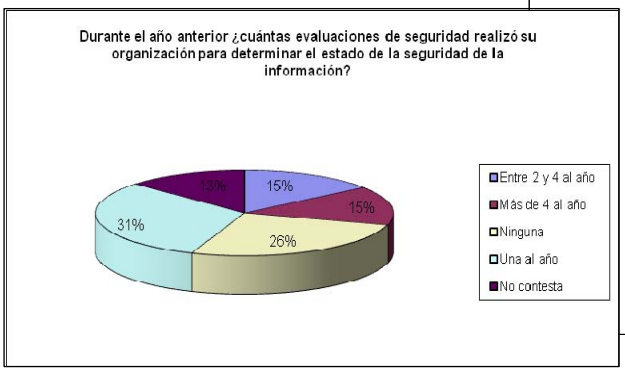



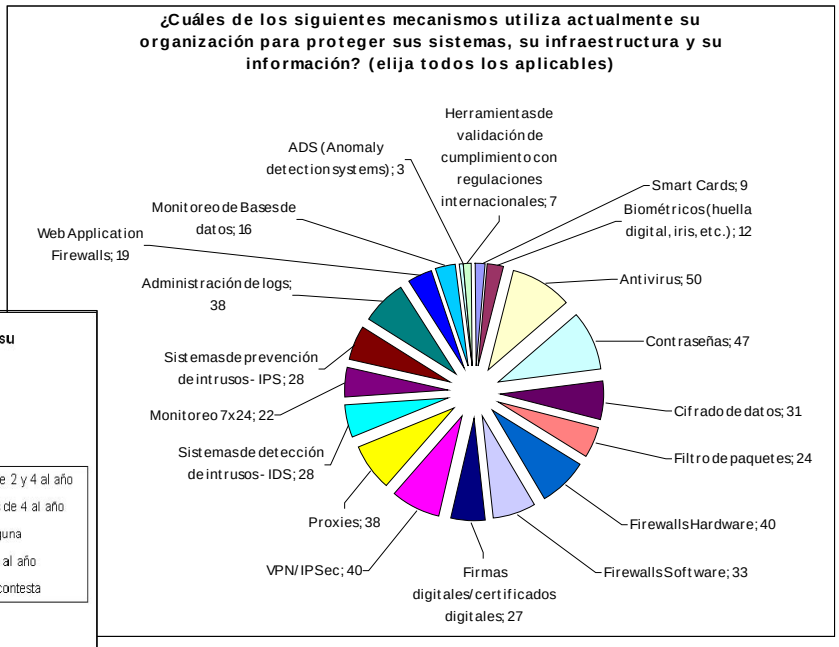

Comentarios generales:

A diferencia de las respuestas recibidas el año pasado, a partir de las cuales podía concluirse que la mitad de los encuestados había tenido entre 1 y 3 intrusiones, este año un 25% señala haber sufrido entre 1 y 3, seguido de un 15% que indica entre 4 y 7 incidentes, mientras que un 30% desconoce la respuesta. Con relación al tipo de incidentes, al igual que el año pasado, los registrados con mayor frecuencia son los virus y la instalación de software no autorizada. Este año le siguen en importancia el phishing, el robo de elementos críticos de hardware y los accesos no autorizados. En cuanto a las preguntas sobre la evidencia digital, al igual que en las encuesta anterior, más de la mitad de los participantes señalan que la organización es consciente de la importancia de la evidencia digital. Sin embargo, sólo un 20% indica que la organización ha aprobado e implementado un procedimiento para su tratamiento. Este porcentaje se encuentra por debajo del registrado el año anterior, que indicaba que un 44% había avanzado en este sentido. Si bien a primera vista, esta observación es desalentadora, debido al tamaño pequeño de la muestra, no pueden tomarse como conclusivas.

### *5. Evaluaciones de Seguridad*

En esta sección se formularon tres preguntas vinculadas a la cantidad de evaluaciones de seguridad realizadas, los mecanismos de protección implementados y la manera en que se tomó conocimiento de las fallas. Se grafica a continuación la primera de las preguntas mencionadas.



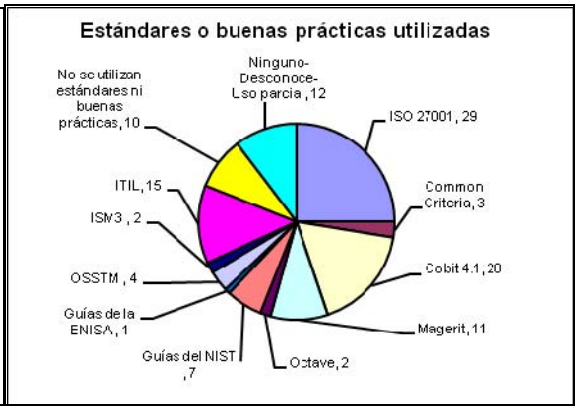

Comentarios Generales

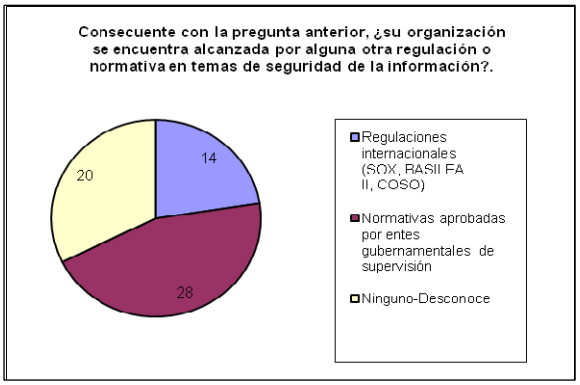
Una de las acciones requeridas por los sistemas de gestión de la seguridad de la información es el monitoreo continuo. Esta actividad resulta importante para corroborar la efectividad de los controles aplicados. En este caso, se observa que la mayoría realiza al menos una evaluación de su seguridad al año, de los cuales un 15% realiza más de 4 y otro tanto, entre 2 y 4. Los valores obtenidos son similares a los del año pasado, habiendo aumentado las respuestas que señalan la realización de más de 4 evaluaciones al año.

Con relación al tipo de mecanismos utilizados para la protección de la información las respuestas también son similares en porcentajes a las registradas el año anterior, siendo las opciones más seleccionadas los antivirus, el uso de contraseñas, las VPN, los proxies y la administración de logs. Cabe acotar que este año se registraron porcentajes algo menores para cada una de ellas. Se aclara que esta pregunta admitía múltiples respuestas.

### *6. Marco de la seguridad*

En esta sección se incluyen preguntas relativas a la existencia de una política de seguridad, los estándares utilizados y las regulaciones que alcanzan a la entidad donde trabaja el participante.

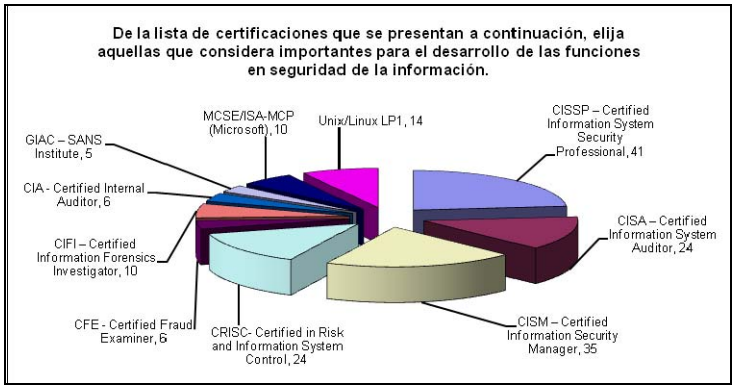



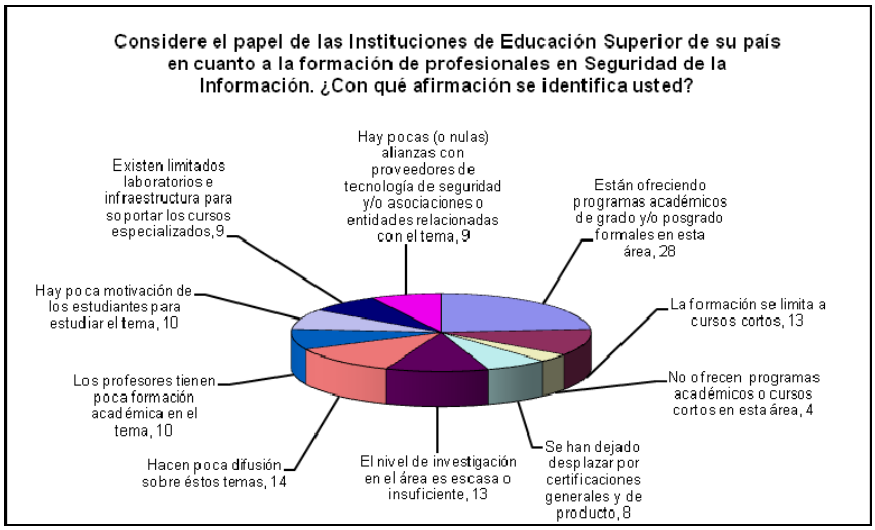

<u>Consideraciones Generales</u>

La definición de políticas es el escalón fundamental para la efectiva implementación de un programa efectivo de seguridad de la información en la organización. Sin embargo, no se observan mejoras en cuanto a la cantidad de respuestas con una política de seguridad escrita, aprobada e informada. Los porcentajes observados son muy similares a los registrados en la encuesta anterior, toda vez que este año algo más de un 50% de las respuestas señalan contar con una política formalizada, un 15% indica que se encuentra en desarrollo y un porcentaje similar responde que la han desarrollado aún. Con relación a los estándares aplicados sigue prevaleciendo la ISO 27001 y el COBIT 4.1 (aunque ambos presentan una proporción menor que el año pasado), seguidos por ITIL y las guías del NIST. Cabe destacar que las normas mencionadas son las más conocidas y respetadas internacionalmente. Respecto a la normativa aplicable, prevalecen aquellas exigidas por los entes gubernamentales de supervisión, seguidas por las regulaciones internacionales, siendo el porcentaje de respuestas recibidas muy similar al registrado en la encuesta anterior.

## *7. Capital intelectual*

En esta sección se engloban las preguntas vinculadas a las certificaciones profesionales y a los programas académicos de formación en seguridad informática.




<u>Comentarios Generales</u>

Aunque con distintos porcentajes y peso relativo es posible observar que las certificaciones destacadas son CISSP, CISA, CISM y CRISC, siendo éstas las más reconocidas en el mercado profesional específico. Cabe destacar con respecto al año pasado, un crecimiento notorio de la Certificación CISM y la aparición de la nueva certificación sobre CRISC, que iguala en valoración a la certificación CISA.

En cuanto a los programas académicos, un 40% indica que se encuentran disponibles mientras que un 25% opina que no se hace suficiente publicidad y que la investigación en la materia es escasa. Respecto al año pasado, ha crecido la percepción respecto a la existencia de programas académicos pero también la opinión respecto a que hay insuficiente investigación.

## Conclusión

Si bien -como se dijo más arriba-, este año registró un marcado aumento en las respuestas recibidas, las mismas aún no resultan suficientes como para configurar una muestra representativa. En consecuencia, este informe debe ser interpretado a la luz del

esta circunstancia. Sin embargo, es posible identificar algunos aspectos que, de acuerdo con nuestra experiencia, caracterizan la situación actual en materia de seguridad informática. De igual manera, la existencia de una encuesta anterior permite realizar alguna observación en cuanto a la evolución mostrada. Siguen a continuación algunos comentarios sobre los análisis realizados:

- El porcentaje del presupuesto de TI asignado a Seguridad Informática sigue siendo escaso, teniendo en cuenta la importancia estratégica que la seguridad tiene para una cada vez mayor cantidad de productos y servicios de TI que prestan las organizaciones
- Frente a las preguntas relativas al reconocimiento de la información como un activo a proteger por parte del personal, y al nivel de concientización respecto a la seguridad informática, se aprecian niveles aún bajos, en particular en cuanto a la percepción de los directivos y autoridades. Este es un aspecto crucial para avanzar en una adecuada protección de los datos y de los recursos de información.
- Se reconoce la importancia de la evidencia digital. Sin embargo, es escaso el número de organizaciones que ha establecido procedimientos para su tratamiento. Este tema de creciente importancia al ser cada vez mayor el número de servicios que se prestan por Internet, debe ser atendido en forma urgente a fin de evitar problemas de diversa índole, especialmente legales, en el futuro.
- A diferencia del año pasado que reflejó un reconocimiento del 70%, poco más del 50% de los encuestados afirmó haber sufrido incidentes de seguridad. En cuanto a la tipificación, sigue siendo alto el porcentaje de instalación de software no autorizado, la presencia de virus y el phishing.
- En cuanto a las Políticas de Seguridad, base de cualquier esquema de protección de los recursos de una organización, sigue siendo bajo el porcentaje que manifiesta contar con versiones formales, documentadas e informadas a todo el personal.
- Las certificaciones más apreciadas en las organizaciones continúan siendo CISSP, CISM y CISA, apareciendo este año CRISC, la nueva certificación de ISACA sobre Riesgo, sugida el año pasado. Se destaca también la mayor importancia otorgada a CISM, como certificación de seguridad de la citada organización.

En la medida en que crezca la cantidad de participantes en futuras realizaciones de esta encuesta, será posible contar con una muestra de mayor tamaño que permita avalar en forma más precisa los resultados observados. De esa manera, será posible conocer mejor qué está ocurriendo en nuestro país y en Latinoamérica en materia de seguridad informática, en procura de contar con una herramienta que contribuya a mejorar el proceso de toma de decisiones en esta área de creciente criticidad para las personas, las organizaciones y los países de la región.

***Marcia Liliana Maggiore.*** *Es Computador Científico de la Universidad de Buenos Aires (UBA) y tiene una certificación internacional en Auditoria de Sistemas (CISA), otorgada por ISACA. Ha concluido la Maestría en Seguridad Informática de la UBA, encontrándose actualmente desarrollando la tesis. Es expositora de temas de auditoría de sistemas, control y seguridad de la información para la certificación internacional CIA (IAIA – Instituto de Auditores Internos de Argentina) y las certificaciones internacionales CISA y CISM (ADACSI – Asociación de Auditoría y Control de Sistemas de Información). En su carrera laboral ha desempeñado los cargos de Gerente de*

*Seguridad Informática, Coordinador del Comité de Seguridad Informática, Gerente de Auditoría de Sistemas y Coordinador de Auditorías de Procesos en la Administración de Seguridad Social de Argentina, Jefe de la División Auditoría de Sistemas en el Banco Nacional de Desarrollo del mismo país y Jefe de Sistemas en la empresa NOVADATA. Es autora de varios artículos publicados en revistas técnicas y coautora del libro "Normas Internacionales y Nacionales vinculadas a la Seguridad de la Información" junto a María Patricia Prandini. En la actualidad es docente en el Postgrado de Seguridad Informática que se dicta en la UBA.*

***Patricia Prandini**. Es Contadora Pública y Especialista en Seguridad Informática de la Universidad de Buenos Aires (UBA) y tiene una Maestría de la Universidad de Illinois, EEUU. Ha terminado de cursar la Maestría en Seguridad Informática en la UBA, encontrándose actualmente desarrollando su tesis. Tiene certificaciones internacionales en Auditoría de sistemas (CISA) y en Riesgo (CRISC) de ISACA. Lideró entre otros proyectos, la implementación de la Infraestructura de Firma Digital de la República Argentina y el ArCERT (Coordinación de Emergencias en Redes Teleinformáticas de la Argentina). Es docente de Auditoría y Seguridad Informática en la UBA, la Universidad Nacional de San Martín y la Universidad Austral. Es presidente del Capítulo Buenos Aries de ISACA y actualmente se desempeña como auditora de Entidades Certificantes en el Estado argentino. Es coautora del libro "Normas Internacionales y Nacionales vinculadas a la Seguridad de la Información" junto a Marcia Maggiore.*