

Informe Anual sobre Ciberdelitos de CSI 2008

Título original: [CSI Computer Crime & Security Survey](#)

Autor: Robert Richardson, CSI Director

Traducción: Raúl Batista exclusivo para [Segu-Info](#)

Fecha Publicación: 06 de diciembre de 2008

Los resultados del estudio sugieren que los ataques, la mayoría de ellos, son menos imaginativos de lo que es posible en teoría. Lo cual es una buena noticia, por el momento.

Hallazgos claves

Los incidentes más costosos fueron aquellos que involucraron fraudes financieros... con una pérdida promedio cerca de u\$s 500.000. El segundo tipo más costoso, en promedio, fue los relacionados con computadoras zombies dentro de la red de la organización, reportando cerca de u\$s 350.000. La pérdida promedio se estableció debajo de los u\$s 300.000.

Los incidentes con virus son los que sucedieron con mayor frecuencia... y ocurrieron en casi la mitad (49%) de las organizaciones encuestadas. Los abusos internos fueron el segundo en frecuencia (44%) seguido por el robo de laptops y otros dispositivos portátiles (42%).

Casi una de cada diez organizaciones informaron haber tenido un incidente con DNS... respecto del 2% del año pasado, algo significativo dado el foco actual sobre las vulnerabilidades en DNS

Veintisiete por ciento de los que contestaron a la pregunta referida a "ataques dirigidos"... dijo que habían detectado al menos un ataque de ese tipo. Donde por "ataque dirigido" se entiende el caso de ataques con malware dirigidos solo a la organización.

La amplia mayoría de los encuestados respondió que tienen (68%)... o están desarrollando (18%) una política formal de seguridad de información. Solo el 1% dijo que no tiene política de seguridad.

Sobre el informe

El [13° informe de seguridad que el CSI](#) preparó en base a las respuestas anónimas de más de 500 profesionales de seguridad, miembros o participantes de conferencias pagas del CSI.

Es una encuesta informal y no es una muestra al azar. El perfil de los consultados sigue mostrando el mismo perfil demográfico que años anteriores, siendo ellos CIOs, CEOs, CSOs, CISOs, Oficiales de Seguridad y Administradores de sistemas.

Quienes responden se desempeñan en organizaciones de todo tipo y tamaño, financiero, consultoría, tecnología de la información, salud, agencias de gobierno, militar, de seguridad, educación, y otros. Organizaciones de 1500 empleados o

más forman la mitad de los participantes y la otra mitad organizaciones medianas y pequeñas. Casi un cuarto fueron organizaciones de menos de 100 empleados.

Aunque los participantes están involucrados, conocen y les preocupa la seguridad, solo la mitad reportó que usan sistemas de administración de logs de seguridad.

El 53% de los encuestados reportó que a seguridad le dedican el 5% o menos del presupuesto total de TI. Significativamente menos que el 61% reportado el año anterior. La seguridad se ve como un problema que abarca más que lo tecnológico, el presupuesto también viene de departamentos de auditoría y legales.

En entrenamiento el 42% dijo que gasta menos del 1% del presupuesto de seguridad en programas de concientización. Si bien hubo cambios respecto al año anterior, en general se observa muy baja inversión en esta materia que tanta importancia se menciona en discusiones.

Justificaciones de negocios

Los medios de justificación económica utilizados para conseguir aprobación de proyectos de seguridad siguen siendo utilizados aunque en contraste con el año 2004 todos han disminuido su utilización. Se deduce que los economicistas no han sido capaces de proveer a los profesionales de seguridad de un modelo dominante para la toma de decisiones. Y aunque algunos practicantes de la seguridad ven útil plantear la pérdida económica potencial frente al costo de prevenirla, en la práctica claramente no es la fuerza predominante para la toma de decisiones.

El nivel de tercerización sigue prácticamente igual a los años anteriores, la mayoría de las tareas de seguridad siguen siendo realizadas internamente. En seguros como medida de mitigación, este año se registra un leve aumento del 29% al 34%.

Frecuencia, naturaleza y costo de las brechas de seguridad

Como en años anteriores (45% en 2007) casi la mitad de los profesionales consultados (44% en 2008) responden que no han tenido incidentes de seguridad, un hallazgo interesante y que muestra la tendencia del grupo consultado interesado por la seguridad. Sin embargo está bastante por debajo del 70% que respondía lo mismo por el año 2000.

En cuanto al número de incidentes, se mantienen similares respecto de años anteriores. El 47% dice que tuvo entre 1 y 5 incidentes, el 14% que tuvo de 6 a 10 y 13% más de 10 incidentes.

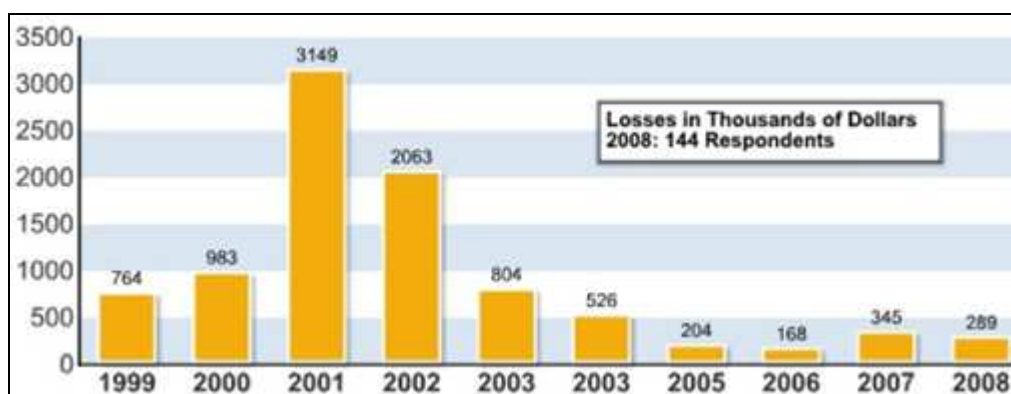
En términos de pérdidas económicas la consulta respecto si fueron causadas por ataques internos o externos, este año aumentó al 51% quienes piensan que no son internas y un 25% les atribuyen a las pérdidas por ataques internos entre 1 y 20% del monto total de pérdidas.

En cuanto a tipo de ataques, desde 1999 siguen siendo cuatro las categorías que son de alta incidencia: 50% reportaron problemas con virus, 44% abusos internos, 42% robo de laptops y 29% acceso no autorizado a sistemas. Las dos primeras categorías vienen cayendo año tras año, y en general también las demás.

De las 18 categorías de incidentes apenas cuatro tuvieron algún aumento.

Table 1	2004	2005	2006	2007	2008
Denial of service	39%	32%	25%	25%	21%
Laptop theft	49%	48%	47%	50%	42%
Telecom fraud	10%	10%	8%	5%	5%
Unauthorized access	37%	32%	32%	25%	29%
Virus	78%	74%	65%	52%	50%
Financial fraud	8%	7%	9%	12%	12%
Insider abuse	59%	48%	42%	59%	44%
System penetration	17%	14%	15%	13%	13%
Sabotage	5%	2%	3%	4%	2%
Theft/loss of proprietary info	10%	9%	9%	8%	9%
from mobile devices					4%
from all other sources					5%
Abuse of wireless network	15%	16%	14%	17%	14%
Web site defacement	7%	5%	6%	10%	6%
Misuse of Web application	10%	5%	6%	9%	11%
Bots				21%	20%
DNS attacks				6%	8%
Instant messaging abuse				25%	21%
Password sniffing				10%	9%
Theft/loss of customer data				17%	17%
from mobile devices					8%
from all other sources					8%

La pérdida económica promedio por incidente ha bajado este año a u\$s 288.000 respecto de los u\$s 345.000 del año pasado. Pero aún está por encima de los u\$s 168.000 a los que había bajado hace dos años, después de 5 años consecutivos de descenso.



Se observa también que cada vez menos de los encuestados que contestan en esta categoría de pérdidas económicas, solo 144 respondieron. Marca una tendencia a no compartir este tipo de información.

Este dato es para tener en cuenta ya que el bajo número que contesta en cada categoría no es suficiente para que se pueda analizar cada una. Dicho esto, la categoría con costos promedios más caros por incidente fue la de fraude financiero con un promedio de u\$s 463.000, seguida por los incidentes con redes bot con un costo informado promedio de u\$s 345.000. Luego la pérdida de información propia y la de clientes con un costo promedio de u\$s 241.000 y u\$s 268.000 respectivamente. Otra categoría como los incidentes por virus reportan un costo promedio de u\$s 40.000 por incidente.

Como el año anterior los profesionales de seguridad notan una mayor profesionalización del ciberdelito y cada vez más es motivado por el dinero más que por alardear.

Las medidas de seguridad que se toman contra los atacantes como firewalls y anti-virus son imperfectas, se basan en detener ataques conocidos. Debido a la sofisticación creciente de los creadores de malware, este enfoque empieza a ser cada vez es menos efectivo. Llegan al punto que pueden superarlo más o menos a voluntad, al menos por un cierto lapso de tiempo.

Los ataques dirigidos ya no son teóricos, son una realidad y este año los reportaron 27% de los encuestados, aunque el año pasado los reportaban el 32%.

Tecnología de seguridad utilizada

Como es de esperar casi todos contestan que utilizan firewalls (94%) y antivirus (97%), un 80% informa que usa antispyware, igual que el año pasado. Por segundo año se consulto por el uso de VPN, 85% lo utiliza.

Table 2: Technologies Used	2008
Anti-virus software	97 %
Anti-spyware software	80 %
Application-level firewalls	53 %
Biometrics	23 %
Data loss prevention / content monitoring	38 %
Encryption of data in transit	71 %
Encryption of data at rest (in storage)	53 %
Endpoint security client software / NAC	34 %
Firewalls	94 %
Forensics tools	41 %
Intrusion detection systems	69 %
Intrusion prevention systems	54 %
Log management software	51 %
Public Key Infrastructure systems	36 %
Server-based access control lists	50 %
Smart cards and other one-time tokens	36 %
Specialized wireless security systems	27 %
Static account / login passwords	46 %
Virtualization-specific tools	29 %
Virtual Private Network (VPN)	85 %
Vulnerability / patch management tools	65 %
Web / URL filtering	61 %
Other	3 %

Auditoría de seguridad y entrenamiento en concientización sobre seguridad

Consultados por como verifican la efectividad de las medidas de seguridad, el 64% dice hacerlo mediante auditorías internas como el enfoque predominante para esto. Pero un 55% dice estar utilizando herramientas automatizadas. Aproximadamente la mitad responde utilizar auditoría externa, monitoreo de correo electrónico y navegación Web.

Respecto del entrenamiento en concientización, un 18% dice no hacerlo, al igual que el año pasado, lo que implica que 4 de cada 5 encuestados realiza entrenamientos, pero un 32% no realiza ninguna medición de la efectividad de este entrenamiento.

Compartir información

Se observa una menor participación en las organizaciones que reúnen información sobre seguridad e incidentes.

Respecto de la primera acción que toman las organizaciones después de un incidente, se aprecia una disminución de quienes lo informan a las fuerzas del orden, sólo el 27% frente al 36% que lo hacía en 2001. La tendencia es hacia identificar por sí mismos al atacante, lo informan así el 60%, hace lo mejor que pueden para emparchar los agujeros el 54% y emparchan el software el 46%.

Quienes no reportan a las autoridades este año principalmente no lo hacen porque creen que los incidentes son algo muy pequeño para tomarse la molestia, le sigue quienes creen que las autoridades no podrán ayudar y recién en tercer lugar quienes piensan que reportarlo será una publicidad negativa.

Nuevas preguntas

Este año se introdujeron nuevas preguntas y una de ellas es respecto de si la organización ha implementado políticas de seguridad formales. Aun no hay suficiente información para saber si esto tiene o no un impacto en menor cantidad de incidentes importantes. Aun así es de destacar que la mayoría de quienes respondieron ya tienen implementadas políticas (formales o no) o las están desarrollando.

Otra pregunta nueva es respecto si la organización tiene una política formal de retención/destrucción de información, cerca de la mitad la tiene y otro cuarto está trabajando en ello.

Otra área donde se está haciendo foco es sobre si es posible mejorar la seguridad si se mejora en los desarrollos de software internos para que se programen con menos vulnerabilidades. Si bien no se ha progresado tanto como con las políticas de seguridad y las de retención de información, más de un cuarto de los que contestaron mencionaron que su organización ya tiene implementado un proceso formal de desarrollo seguro.

Preocupaciones generales

Hace dos años se consulta respecto de cuales creen que serán los asuntos críticos en seguridad que se piensan podrán enfrentar en los siguientes dos años. Las principales preocupaciones planteadas en las respuestas de este año giraron sobre: la protección de la información de los clientes, la amenaza de los dispositivos móviles y los inalámbricos y el área general de preocupaciones de administración: como argumentar sobre la seguridad a la alta dirección, retener al personal valioso, mantener los niveles de seguridad si baja el presupuesto.

Comentarios finales

Las pérdidas financieras después de un aumento el ante año, volvieron a bajar, pero no se cree que será así indefinidamente.

Se estima que será de preocupación los ataques que se hacen posibles a medida que nos movemos hacia una Web más orientada a servicios, pero estas amenazas aun no se ven difundidas, aun.

Aún son de utilidad algunas herramientas claves para defensa perimetral y aplicadas correctamente ayudan a bajar las pérdidas, pero tienen sus límites.

Este informe ha sido traducido por Raúl Batista
en forma exclusiva para [Segu-Info](http://www.segu-info.com.ar)