RESPUESTAS SiC

Madrid: 24 de junio de 2008
(Hotel NH Eurobuilding)

Barcelona: 26 de junio de 2008
(Hotel Rey Juan Carlos I)

Prevención de fugas y pérdidas

La información, bajo control

Inscripciones:

- Acceso gratuito previa solicitud de inscripción.
- Solicitud: www.revistasic.com/respuestassic

> AFORO LIMITADO

Organiza:

Revista SiC seguridad en informática y comunicaciones

Copatrocinan:

Check Point SOFTWARE TECHNOLOGIES LTD. · McAfee · RSA The Security Division of EMC · symantec. · TREND MICRO · WEBSENSE · zitralia

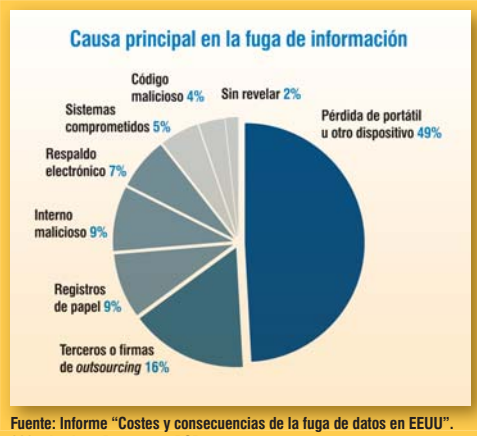
La información, bajo control

La pérdida y el robo de información corporativa (financiera, bancaria, comercial, industrial, de adquisiciones, recursos humanos, planificación estratégica, propiedad intelectual...) y de datos de carácter personal (ciudadanos, empleados, clientes, accionistas, proveedores...) que se tratan en las organizaciones, y que muy por lo común también se localizan en el medio electrónico (documentos/archivos de texto, hojas de cálculo, presentaciones en distintos formatos, gráficos, imágenes, sonido...) sin protección (restricciones para su creación, límites de acceso por terceros...) y que generalmente no están asociados de manera robusta con su autor y con los usuarios que pueden tratarlos, plantea un problema creciente en orden al cumplimiento de legislaciones diversas y, obviamente, puede socavar, si se produce y se divulga, la buena reputación o la competitividad en los mercados.

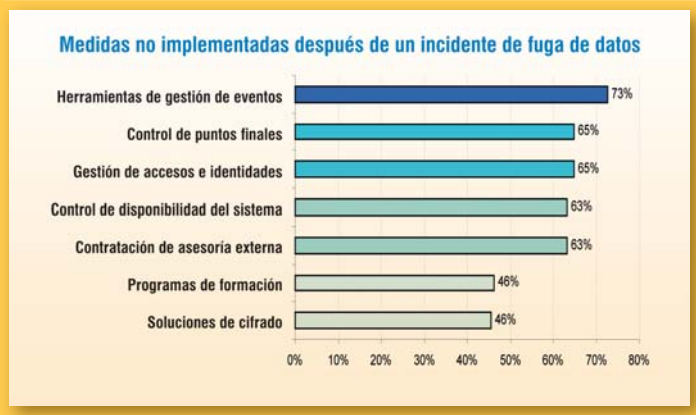
El enquistamiento del problema se agrava si tenemos en cuenta el enorme potencial de, por ejemplo, el servicio de correo electrónico y los anexos como canal de fuga, y también la proliferación del uso, sin las debidas medidas de seguridad técnica implantadas, de equipos y dispositivos de cliente que incrementan la exposición al riesgo (ordenadores portátiles y de sobremesa, impresoras, escáneres, teléfonos móviles, PDA, smartphones, Blackberries, iPhones, CD-Rom, DVD, memorias flash, cintas...) por sus crecientes facilidades de acceso a aplicaciones y conectividad con la que se han dotado y se dotarán a algunos de ellos.

A lo mencionado se suma un hecho incontrovertible: que la información de valor es un bien codiciado por los delincuentes, a quienes puede proporcionar en última instancia dinero y diversos medios para obtenerlo: venderla al mejor postor, chantajear a la organización; o dañar el buen nombre y afectar a los negocios de la corporación, divulgándola. Protegerla es, pues, una obligación de todos, y particularmente de los primeros ejecutivos, ya que de una inacción demostrable en este particular podrían deducirse responsabilidades de distinto calado. Es menester, aquí, un buen engranaje entre las áreas de seguridad, auditoría y cumplimiento normativo.

Fugas y pérdidas: el reto de la protección



Fuente: Informe "Costes y consecuencias de la fuga de datos en EEUU". 2007. Instituto Ponemon y PGP



Fuente: Informe "Impacto en el negocio por fuga de datos". 2007. Instituto Ponemon y Scott & Scott

El coste de la fuga de datos, a partir de tres ejemplos de compañía

Categoría	Descripción	Coste por registro: Compañía A: Incidente de perfil bajo en una industria no regulada	Compañía B: Incidente de perfil bajo en una industria regulada	Compañía C: Incidente de perfil alto en una industria altamente regulada
Descubrimiento, notificación y respuesta	Asesoramiento legal externo, notificación postal, llamadas, *call center* y ofertas de descuento de productos	50$	50$	50$
Pérdida de productividad de la plantilla	Reasignación de tareas a los empleados	20$	25$	30$
Coste de oportunidad	Pérdida de clientes y dificultades para conseguir nuevos clientes	20$	50$	100$
Sanciones legales	FTC, PCI, SOX	0$	25$	60$
Indemnizaciones	Los tribunales pueden pedir disponer de estos fondos en caso de que las brechas sean descubiertas	0$	0$	30$
Seguridad adicional y requisitos de auditoría	Los requisitos de auditoría y seguridad aumentan como resultado de un incidente de este tipo	0$	5$	10$
Otras responsabilidades	Costes de reemplazo de tarjetas de crédito. Penas civiles si se encuentran indicios de fraude específico relacionado con la fuga de datos	0$	0$	25$
Coste total por registro		90$	155$	305$

Fuente: Informe "Calculando el coste de una brecha de seguridad". 2007. Forrester Research.

Contenido

La estructura prevista de este VIII Respuestas SIC incluirá tres bloques. En el primero, conformado por dos ponencias, a cargo de las compañías **PricewaterhouseCoopers** y **Davinci**, se tratará de enfocar este creciente problema y vislumbrar una posible solución sistemática, que pasa por la realización de una clasificación de la información en función de su criticidad para el negocio, la actividad y frente al riesgo de incumplimiento de leyes y normas (en estos frentes, dicha clasificación suele atenerse preferentemente al criterio de confidencialidad), y al establecimiento de controles internos sobre la información, los usuarios y los posibles medios de fuga.

El segundo bloque consiste en mostrar cuáles son, hoy día, las aproximaciones tecnológicas de la industria para ayudar a que los profesionales de las organizaciones puedan controlar el correcto acceso, uso, tránsito y seguimiento de su información corporativa. Para ello siete compañías de referencia en la materia (**Check Point**, **McAfee**, **RSA**, **Symantec**, **Trend Micro**, **Websense** y **Zitralia**) mostrarán el estado del arte de sus catálogos especializados para atender este frente de protección, sea mediante soluciones globales, orientadas a la red o a los puestos finales.

El tercer y último epígrafe lo conformará una mesa redonda en la que usuarios de organizaciones de nuestro país –en esta ocasión cualificados expertos del área de los riesgos y la seguridad de la información de **Bankinter**, **Caja Madrid** y **Gas Natural**– debatirán sobre su visión al respecto, tanto en lo concerniente a los límites de los escenarios actuales como a las necesidades futuras, que, a su entender, demandará el intercambio informativo y de actividad mercantil de las entidades públicas y privadas que operan con TIC, con un enfoque realista y moderno del uso autorizado de la información, y su pertinente seguimiento y control.

Programa

CLAVES PARA DECIDIR

09:00h. Acreditación y entrega de documentación

09:30h. **La necesidad de una clasificación de la información y del establecimiento de controles internos sobre la información y los usuarios.**

Elena Maestre García, Directora de los Servicios de Seguridad de la Información de PricewaterhouseCoopers.

10:00h. Coloquio.

10:05h. **Consideraciones en el despliegue de soluciones tecnológicas de protección globales, orientadas a la red o a los puestos finales.**

Enrique Aristi Rodríguez, Director de Operaciones de Davinci.

10:35h. Coloquio.

APROXIMACIONES TECNOLÓGICAS DE LA INDUSTRIA

10:40h. **Check Point.**

Eusebio Nieva Hernández, Director Técnico.

11:00h. **McAfee.**

Blas Simarro Lorite, Director Técnico.

11:20h. **RSA.**

Manuel Lorenzo Vista, Ingeniero de Sistemas Senior Iberia.

12:00h. **Symantec.**

Daniel Arnanz Yagüe, Consultor Senior Preventa.

12:20h. **Trend Micro.**

Gabriel Agatiello, Responsable de Producto.

12:40h. **Websense.**

Karen G. Cordero, Directora Regional para España y Portugal.

11:40h. Pausa-café.

13:00h. **Zitralia.**

Manuel Arrevola Velasco, Director General Comercial.

13:20h. Coloquio general.

MESA REDONDA

13:30h. **La visión de los usuarios. Escenarios actuales, limitaciones y necesidades futuras.**
Participantes:

Julio San José Sánchez, Gerente de Seguridad Informática de Bankinter.

Javier Sevillano Izquierdo, Responsable de Infraestructura Tecnológica. Departamento de Seguridad Informática de Caja Madrid.

Andreu Bravo Sánchez, Responsable de Seguridad Tecnológica de Gas Natural.

14:30h. Almuerzo para todos los asistentes.

* Revista SIC se reserva el derecho a modificar el contenido o los ponentes de este programa si las circunstancias así lo requieren.

El control del riesgo de pérdida o robo de información de valor y la implantación de medidas de seguridad obligatorias en los medios TIC que la organización pone a disposición de sus directivos y empleados, se configura como el gran reto para los departamentos de seguridad TIC, al obligarles a proteger la información sin perturbar la operativa de negocio.

- ¿Se ha llevado a cabo en su organización una clasificación de la información, en orden a su criticidad para los negocios y actividades, atendiendo al criterio de confidencialidad, soportada por un sistema de permisos de acceso de usuarios?
- ¿Conoce con el debido detalle en qué medios y formatos se encuentra o puede encontrarse la información de valor para la entidad?
- ¿Contempla su organización el uso de mecanismos que permitan asociar de modo fiable la posibilidad de crear y tratar documentos electrónicos con la identidad de sus autores y receptores?
- ¿Se puede hacer un seguimiento de la creación y uso que el personal da en la organización a la información de negocio contenida en documentos de texto, hojas de cálculo, presentaciones, imagen y sonido...?
- ¿Hay implantadas medidas tecnológicas de control y restricción de uso sobre llaves USB, CD-Rom y otros dispositivos que pueden grabar información, y límites en sus posibilidades de conectividad?

Los incidentes de fuga de información por terceros y la aceleración de los costes por pérdida de negocio, en ascenso

Por tercer año consecutivo, el Instituto Ponemon presentó a finales de 2007 las conclusiones de un nuevo estudio que examina los costes y consecuencias derivadas de los incidentes de fuga de datos en corporaciones, que, a pesar de centrarse en una escasa muestra, compuesta por 35 organizaciones norteamericanas –con incidentes en los que se vieron comprometidos entre algo menos de 4.000 registros y más de 125.000, procedentes de 15 sectores de actividad diferentes–, adquiere valor por las habituales reticencias que las firmas víctimas de estos episodios tienen a comunicarlos abiertamente.

En este sentido, entre la información que aporta el estudio es destacable el hecho de que, además de seguir aumentando los costes medios totales de estos incidentes, situándose en 197 dólares por registro comprometido (un 9% más que en 2006 y un 42% más que en 2005), y en más de 6,3 millones de dólares por incidente (entre un mínimo de 225.000 dólares y casi 35 millones de dólares), los costes corporativos que más se aceleraron fueron los derivados de la pérdida de negocio, aumentando en más de un 30%, con una media de 4,1 millones de dólares o 128 dólares por registro comprometido. Así, la pérdida de negocio supuso en 2007 un 65% de los costes de fuga de datos, comparado con un 54% en 2006.

Igualmente destacable es el hecho de que los incidentes de seguridad protagonizados por terceras organizaciones, como servicios profesionales, compañías de *outsourcing*, fabricantes y socios de negocio en posesión de la información y responsables de su protección fueron señalados [illegible] un 40% de los participantes en el estudio, aumentando así un 29% respecto [illegible] un 21% respecto [illegible] 2005. De hecho, las fugas de información de [illegible] más costosas [illegible] compañía, con un [illegible] en 2007, del 100% de incidentes [illegible]

Algunas [illegible] participantes tras una brecha de [illegible] que finalizaron [illegible] en 2007, [illegible]

- ¿Se han establecido medidas de confidencialidad no optativas que preserven la información tratada por los directivos y empleados que usan ordenadores portátiles ante robo, pérdida o intento de uso no legítimo?
- ¿Está protegida la información de valor que se trata en el parque móvil corporativo ante sustracciones, robos o intentos de copia?
- ¿Supone una fuente de riesgo para la información corporativa clasificada el uso indiscriminado de correo electrónico con posibilidad de portar documentos adjuntos?
- ¿Se pueden crear libremente en la empresa documentos electrónicos con información de valor, sin que exista un control exhaustivo de quién los crea, quiénes los usan y para qué?
- ¿Qué volumen de documentos electrónicos con información de valor para el negocio transita de dentro hacia fuera de la compañía?

RESPUESTAS SIC

Prevención de fugas y pérdidas. La información, bajo control.

LUGAR Y FECHAS

- **MADRID:** 24 de junio de 2008
  Hotel NH Eurobuilding.
  C/. Padre Damián, 23. 28036 Madrid
- **BARCELONA:** 26 de junio de 2008
  Hotel Rey Juan Carlos I.
  Avda. Diagonal, 661-671. 08028 Barcelona

ORGANIZA

Revista SIC. Ediciones CODA.
C/. Goya, 39. 28001 Madrid
Tel.: 91 575 83 24
info@revistasic.com www.revistasic.com

SOLICITUD DE INSCRIPCIÓN GRATUITA

El procedimiento para la solicitud de la inscripción es vía web mediante la cumplimentación de un formulario. Al ser el aforo limitado, la inscripción se cursará por riguroso orden de fecha de entrada de solicitud.

Sitio web: www.revistasic.com/respuestassic

- Una vez realizada la solicitud, la organización le informará –por razones de limitación del aforo– si ha quedado inscrito o no.
- En ningún caso se admitirán más de dos inscripciones de profesionales de una misma compañía.
- La sesión incluye documentación, café y almuerzo.