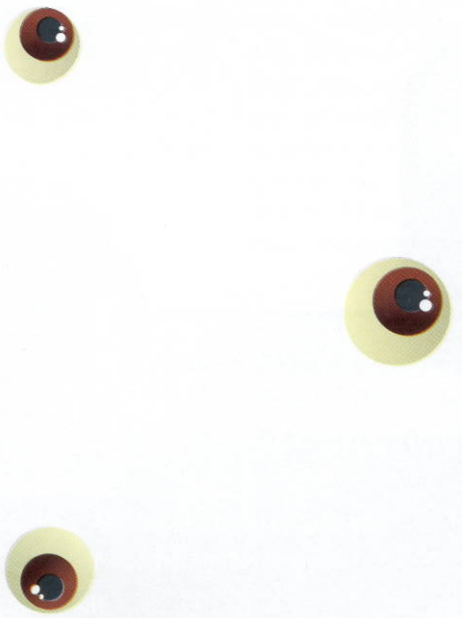


Dónde poner

El manejo de la seguridad informática en las empresas oscila entre las preocupaciones y la falta de presupuesto y atención por parte de la dirección. Dos encuestas revelan sorpresas sobre cómo se protegen las compañías.

Por César Dergarabedian

La figura del CISO (Chief Information Security Officer) se asemeja hoy a la del dios romano Jano, que tenía dos caras mirando hacia ambos lados de su perfil. Según se desprende de dos encuestas difundidas este año, en el caso de la Argentina el responsable de las políticas de seguridad informática tiene que apuntar su mirada vigilante tanto a las amenazas externas como a las que provienen del propio entorno, pero en un contexto donde aún tiene problemas para reportar a la alta gerencia.

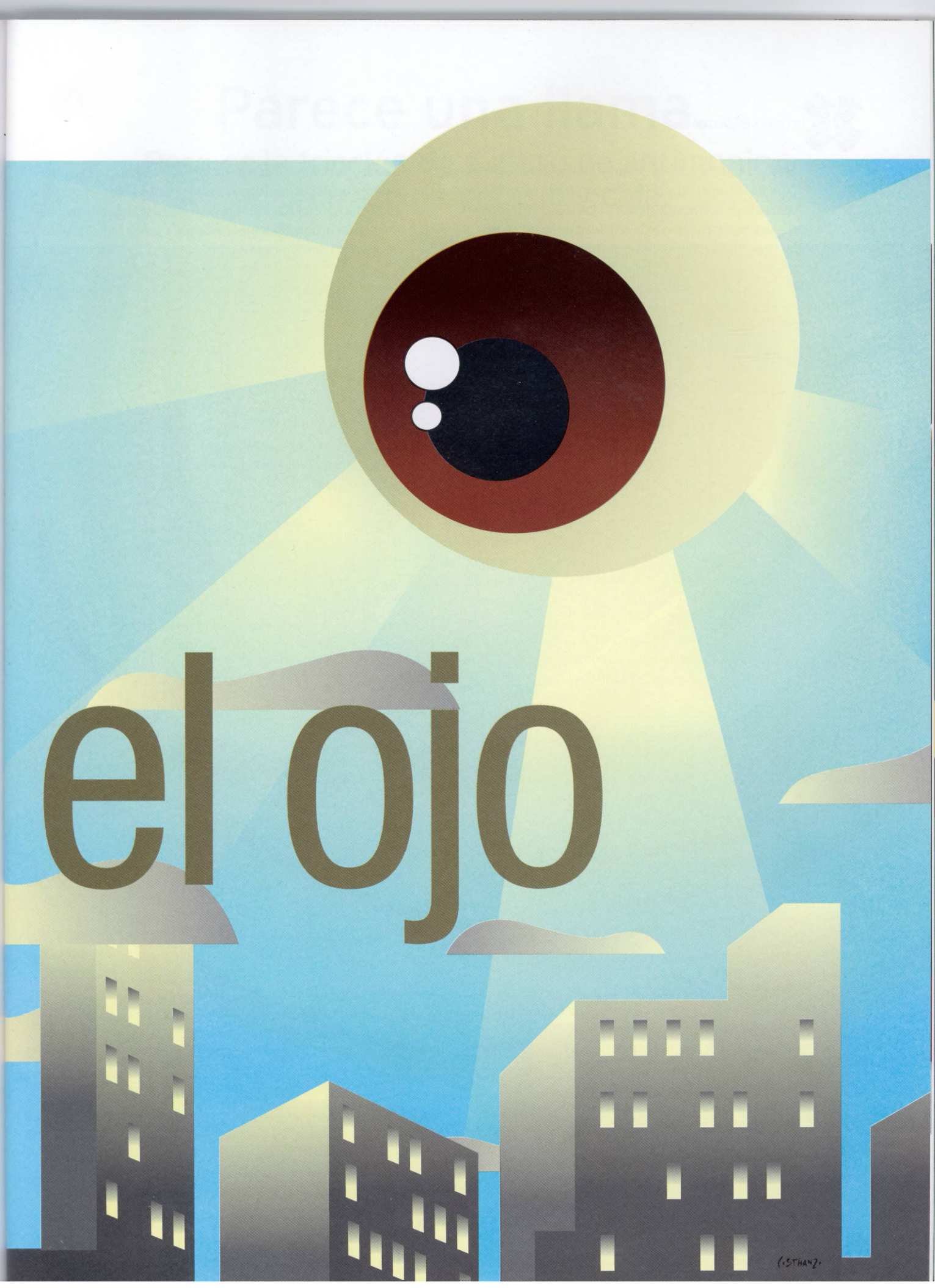
La Encuesta de Seguridad de la Información 2009, realizada por PricewaterhouseCoopers (PWC), afirma que el 79 por ciento de las compañías estableció procesos formales de seguridad de la información, pero sólo el 29 por ciento tiene un director a cargo del tema. En 2008, los ataques más comunes fueron la explotación de datos y redes y los incidentes perpetrados a través del correo electrónico. Los empleados fueron la principal fuente de incidentes, seguidos de cerca por los ex empleados y los "hackers".

Otra investigación, la 6ª Encuesta Anual de Seguridad Global en la Industria Financiera, realizada por Deloitte, apunta a una incoherencia: en la Argentina, el 85 por ciento manifestó poseer una estrategia de seguridad, pero sólo el 40 por ciento sostuvo que está alineada con el negocio y apenas un 15 por ciento emplea métricas para evaluar la gestión y el rendimiento de las medidas de seguridad. Las "restricciones presupuestarias" aparecen como el principal obstáculo para cumplir con las estrategias planteadas.

A punten al e-mail

Sergio Gamba, gerente de Sistemas de Clarín, coincide con los diagnósticos de las dos consultoras sobre la fuente de los ataques. "Los incidentes más habituales con respecto a la seguridad informática provienen del correo electrónico y son nuestros usuarios los principales damnificados", describe el hombre del principal multimedio del país.

Fabio Gasparri, responsable del área de tecnología de la desarrolladora de software Hexacta, también apunta sobre los correos electrónicos: "Los principales incidentes que hemos tenido provienen de ataques de virus recibidos a través de e-mails".


el ojo

Marcelo Giménez, Chief Security Officer de Global Crossing para Latinoamérica y el Caribe, considera como "lógico" al resultado de las investigaciones, y afirma que "lo más cotidiano y representativo es la actividad de spam, técnica que se utiliza para intentar propagar diversos tipos de ataques". Puntualiza que el phishing es "el más crítico y el que mayor seguimiento requiere del sector". Giménez recuerda que este año el ataque del gusano Conficker "no representó un problema significativo en el desenvolvimiento del negocio", aunque "su relevancia mediática generó mucha expectativa, obligando a verificar los controles con el fin de disminuir su posible impacto". Respecto de la actividad detectada en el backbone público de clientes de este operador de telecomunicaciones, se destacan "los incidentes de ataque de fuerza bruta, los intentos por vulnerar sistemas y la descarga de software ilegal".

Sin embargo, desde la aseguradora Allianz Argentina tienen una visión distinta. Daniel Marino, jefe de Seguridad de la Información de esta compañía, afirma que no han cambiado mucho las cosas en el último tiempo. "No hemos sufrido incidentes de seguridad que afecten en forma significativa el desarrollo normal de las operaciones", sostiene.

Controles internos

Diego Taich, gerente de Servicios de consultoría de IT de PWC, apunta al frente interno de las organizaciones como uno de los principales orígenes del fraude: "En cuanto a la autoría de los incidentes de seguridad, casi un 45 por ciento corresponde a empleados o ex empleados, quienes eventualmente tienen oportunidades por encontrarse en una posición de 'confianza' o tener conocimiento adecuado de los procesos y tecnologías utilizadas para acceder o alterar información sensitiva de la organización a través del mal uso o abuso de los medios tecnológicos". Taich agrega el factor de motivación: "Por ejemplo, presión laboral, desvinculación en malos términos o posible pérdida de empleo, cuya consecuencia en algunos casos es la tentación de cometer actos irregulares y fraudes".

Según PWC, el 54 por ciento de las organizaciones en el mundo tiene personal dedicado a monitorear el uso de Internet y de los activos informáticos por parte de los usuarios. Desde Swiss Medical Group, Gustavo Quevedo, gerente corporativo de Seguridad Informática, Auditoría Interna y OyM de este holding de centros de salud, coincide: "Constantemente monitoreamos el uso de Internet ya que éste es tomado como una herramienta de trabajo. Analizamos desde el punto de vista de seguridad los archivos que contienen los e-mails para la detección temprana de virus y ataques. Y también tenemos una herramienta de antispam".

Gamba, de Clarín, marca una evolución en esta cuestión. Antes de 2004, "el uso de Internet era prácticamente libre y, como suele suceder, el ancho de banda nunca alcanzaba. Estábamos en pleno proceso de renovación tecnológica y no podía-

"Los incidentes más habituales provienen del correo electrónico y nuestros usuarios son los principales damnificados"
SERGIO GAMBA, gerente de Sistemas de Clarín

Foto: Gustavo Fernández

Principales incidentes de seguridad en las empresas argentinas

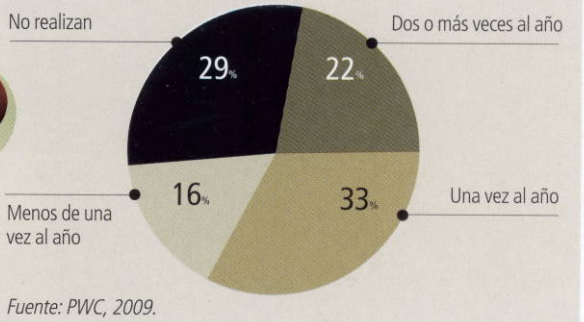
Fuente: PWC, 2009.

claveS

- Realizar una correcta inversión en seguridad requiere el conocimiento preciso del lugar donde residen los mayores riesgos dentro de la organización.
- Luego del diagnóstico, se deben concentrar los gastos de seguridad en las áreas detectadas como críticas.
- Las tecnologías de seguridad serán más efectivas en la detección de incidentes en la medida en que se invierta también en los procesos críticos.
- En la Argentina, la implementación de soluciones de Identity Management es todavía incipiente, porque resulta muy complejo demostrar el ROI ante la alta dirección.

mos implementarlo sin una nueva política que incluyera también un fuerte cambio cultural dentro de la organización". Hoy cuentan con "una política de seguridad alineada con la necesidad de cada grupo de usuarios". En el multimedio tienen una combinación de herramientas de open source y políticas incorporadas dentro de las diferentes aplicaciones.
Marino, de Allianz Argentina, explica que el uso de Internet es "regulado y monitoreado". Para ello, definieron tres tipos de listas de navegación: una negra para los sitios prohibidos, otra blanca de sitios permitidos (extensiones org, .edu, .gob, entre otras) y una gris para el resto de los sitios. "Periódicamente se generan reportes de navegación que informan la categoría de los sitios accedidos", dice el ejecutivo.
En Hexacta apuestan más a un "uso responsable y eficiente de los recursos, y hasta ahora —según Gasparri— nos ha dado muy buenos resultados. No hay un control sobre el contenido, aunque sí hacemos monitoreo del uso de ancho de banda para garantizar que los proyectos tengan un nivel de servicio de Internet adecuado". Además del monitoreo existen reglas de 'traffic shaping' que limitan el uso de ancho de banda, o que lo restringen a determinados horarios para evitar tener problemas de performance en los proyectos.

Empresas que realizan evaluaciones de riesgo en la Argentina



Fuente: PWC, 2009.

Brechas

Las implementaciones de seguridad en procesos críticos también afectan al manejo de dispositivos móviles. Quevedo, de Swiss Medical, explica que con ese fin implementaron "herramientas de monitoreo, detección de intrusos, firewall, proxy, filtrado de contenido, comunicaciones seguras, protección de documentos y de e-mails". En Allianz Argentina, según Marino, limitaron el uso de los Blackberry con "denegación del uso de Bluetooh y de instalación de software". Además, aplicaron un esquema de teletrabajo para algunos empleados, utilizando VPNs bajo las modalidades Ipsec y SSL.
En Hexacta, los routers Wi-Fi están protegidos con clave de 128 bits y los usan sólo el personal autorizado. En Global Crossing implementaron agentes de control, certificados digitales y monitoreo de comportamientos anómalos, entre otros controles. Sin embargo, Giménez asegura que procuran "por sobre todo la concientización de los usuarios, que es prioritaria en cuanto la seguridad en el uso de estos dispositivos".
En Clarín, Gamba destaca el caso de las notebooks, que tienen "un uso intensivo". Estas portátiles poseen "exactamente el mismo nivel de seguridad que las estaciones de trabajo y estamos en pleno proceso de incorporación de un software para encriptación de su contenido en caso de pérdida o robo". El multimedio cuenta con 300 Blackberry. "El servidor de Blackberry está dentro de nuestra red, con un esquema de comunicación cifrado que nos agrega mayor seguridad. Si bien RIM (Research in Motion, proveedor de los equipos) está en el medio del proceso de comunicación, decidimos adoptar esta forma de administrarlos", detalla Gamba.
Los estudios de PWC y de Deloitte advierten que hay una brecha significativa entre el gasto en seguridad y los objetivos del negocio. Además, señalan que el CISO suele tener problemas para reportar a la alta dirección. Según Taich, "en algunos casos, la falta de un lenguaje común y las percepciones diferentes que tienen CEOs y CFOs con respecto a los responsables de la seguridad informática colaboran en la generación de la brecha. Los CISOs son quienes están en el frente de batalla de la seguridad, cercanos a conocer cómo se gasta el dinero y, por lo tanto, en una buena posición de observación para determinar la brecha entre

"El uso de Internet en la compañía está regulado y monitoreado"
DANIEL MARINO, jefe de Seguridad de la Información de Allianz Argentina

Foto: Gustavo Fernández

el gasto en seguridad y los objetivos de negocio. Perciben que esta brecha es importante. Tienen la sensación de que se realizan fuertes inversiones en temas de cumplimiento regulatorio, pero dejando de lado otros temas". El analista de PWC afirma que para alcanzar un mejor alineamiento entre el negocio y el gasto en seguridad hace falta "incorporar prácticas de seguridad que consideren al riesgo de forma integral — es decir, cualquier factor que pueda atentar contra los objetivos del negocio—, estimular la inversión en seguridad como soporte al cambio (acompañando la evolución del negocio) y asegurar un alineamiento de los ejecutivos y de las expectativas en cuanto a la contribución que la seguridad debería hacer al negocio".

Andrés Gil, socio de Enterprise Risk Services (ERS), y Claudia Minzi, gerente de ERS de Deloitte, observan que a la seguridad informática "se la sigue asociando con temas técnicos del área de Sistemas o de Tecnología y aún no se asocia directamente como un tema de negocio". Si bien reparan que esta tendencia se está revirtiendo "de a poco" y en parte motivada por la regulación del Banco Central, "aún sigue estando en la mente de los líderes del negocio como un aspecto técnico". Y remarcan: "A medida que los incidentes o problemas de seguridad se suceden, las organizaciones toman real dimensión de la importancia que la seguridad tiene para el negocio; es entonces cuando la percepción cambia y, en consecuencia, también la asignación de recursos y de prioridades".

Otro aspecto a mejorar, según ambos analistas, es la comunicación de las áreas de seguridad hacia el negocio, ya que se puede lograr mayor compromiso de la alta dirección". A su juicio, "en la medida en que el mensaje sea planteado a nivel ejecutivo y que los controles de seguridad estén enfocados a cubrir los riesgos de seguridad más sensibles para el negocio, el CISO tendrá más visibilidad en la organización y su nivel de dependencia podrá cambiar".

Quevedo, de Swiss Medical Group, muestra otra visión: "Hacemos un análisis detallado de los riesgos que debemos mitigar y, en base a eso, realizamos un presupuesto que presentamos a la Dirección General. Hasta ahora han sido aprobados". Gamba, de Clarín, coincide: "Es un tema estratégico, no sólo al nivel de la gerencia general sino también dentro del Grupo Clarín. En base a nuestro presupuesto, la porción dedicada a seguridad informática nos permite cumplir con los objetivos de negocio de la empresa". Giménez, de Global Crossing, apunta que "Estados Unidos sigue el criterio de seguridad del NSA (Network Security Agreement), por lo cual los lineamientos de la empresa son uniformes en todo el mundo".

Los analistas de Deloitte concluyen: "La estrategia de seguridad quizá sigue siendo un aspecto más vinculado al cumplimiento de un requisito regulatorio que a un lineamiento para el negocio. A medida que el área de seguridad tenga más visibilidad ante la alta gerencia, definir la estrategia y evaluar su cumplimiento con métricas de gestión será un aspecto relevante, no ya para el área de seguridad sino para toda la empresa". ■