El robo de equipo portátil en Costa Rica

Fabián Escalante Zamora[1]

Resumen

Muchos usuarios de computadores que viajan por negocios confían en sus "notebooks" y PDAs ("Personal Digital Assistants"), porque son pequeñas y fácilmente transportables. Pero mientras esas características las hacen populares y convenientes, también las convierten en un blanco ideal para los ladrones. Aunque hay formas físicas de proteger su "notebook", PDA u otro dispositivo portátil, no hay garantía de que no será robado. Después de todo, tal como el nombre lo sugiere, los dispositivos portátiles son diseñados para ser fácilmente transportados. El robo en sí, es frustrante e inconveniente, pero la exposición de la información del dispositivo puede tener serias consecuencias también. Este artículo analizará los principales medios que existen para prevenir la sustracción de equipo portátil, así como los medios existentes en el mercado para indemnizar las pérdidas y daños sufridos al ser víctimas de robo.

Palabras clave

Robo de equipo portátil / Seguros de equipo electrónico / Medios para la recuperación de equipo portátil / Equipo portátil en las empresas

Abstract

Many computers users that travel due to their business trust their notebooks and PDAs because they are small and easily transported. But while those characteristics make them popular and advisable, they also become ideal targets for the thieves. We can find many ways to physically protect notebooks, PDAs or another portable devices, but there is no robbery prevention guarantee. After all, as their name suggests, the portable devices are designed to be transported easily. A robbery is frustrating and inconvenient, but the loss of the information can also have serious consequences. This article will analyze the principal methods that exist to prevent the robbery of portable equipment and the method used to compensate the loss and damages suffered by a robbery victim.

Key words

Theft of portable equipment / Electronic equipment insurance / Methods to recover stolen portable equipment

Cada día más personas son contagiadas con la magia existente en los dispositivos portátiles, ya sean estos un teléfono celular, una computadora portátil o una agenda electrónica, todos son artículos cada vez más buscados por un público que desea contar con su conveniencia, su comodidad por ser portátiles, su poder de desempeño y hasta, por qué no, con el prestigio que socialmente

[1] Ingeniero en sistemas, ULACIT.

se adquiere al contar con uno de ellos. Tal contagio se ve reflejado en cifras de ventas que alcanzan los 400 millones de dispositivos portátiles vendidos en Estados Unidos al año.

Sin embargo, muchas de estas unidades son perdidas por sus dueños en hoteles, taxis, restaurantes y conferencias, entre otros; algunos tienen la suerte de recuperar su preciado equipo, pero la gran mayoría no es tan afortunada y ve cómo su esfuerzo se pierde en solo segundos.

Otro alto porcentaje son robados, muchos por compañeros de trabajo, personal encargado de eventos o cualquier persona que, aprovechando un simple momento de descuido, ven realizados sus sueños de contar con una computadora portátil; también existen los ladrones profesionales, quienes conforman equipos para robar estos artículos con el propósito de revenderlos a una porción de su costo real.

“En cada uno de estos robos o pérdidas, generalmente se toma por valor únicamente el costo que la unidad tiene en ese momento en el mercado; no obstante, en la mayoría de los casos, el verdadero valor se ve reflejado en la información contenida en cada uno de ellos”, comenta Orlando Soto, gerente general del Grupo Financiero Acobo, quien además agrega: “Para mí y para mi empresa sería difícil poder estimar el valor de la información que manejo en mi computadora portátil, mi teléfono celular o mi agenda electrónica, ya que en ellos mantengo información vital sobre el estado actual de la compañía y, más importante aún, los diferentes estudios que realizamos para posibles nuevos negocios”.

Ante esta perspectiva, se infiere que el valor más representativo de los equipos portátiles no se encuentra en el precio que este tiene en el mercado, sino en la información que dicho dispositivo almacena.

Es por ello que se hace sumamente importante contar con una tecnología o medio que deje una ventana de oportunidad para la recuperación del equipo que es robado o para, al menos, poder destruir la información que en ellos se contiene.

Un buen mercado para el hampa

El valor de una computadora portátil puede llegar, por ejemplo, hasta los US$5.000, y si bien es cierto que este valor solo se paga por artículos nuevos, no es menos real que un delincuente puede vender estos ordenadores en una tienda de computación, en algún aviso clasificado o mediante un sitio de subastas por Internet, colocando fácilmente hasta la mitad del valor original de cada artículo.

Pero, además, “este “negocio” delictivo es muchísimo más rentable que cualquier otro hurto –como el carterismo– pues brinda más “ganancias” pero con un riego muy

similar, pues solo se necesita ubicar el momento en que la víctima esté distraída para efectuar el arrebato, sin necesidad de usar armas que puedan significarle al delincuente un riesgo de perder la vida o de ir a prisión, pues "la mayoría de los delincuentes profesionales sabe que las penas por un delito contra la propiedad son menos severas que las de un delito contra una persona" comenta el oficial del Organismo de Investigación Judicial (OIJ), Gustavo Garita.

Muchas personas creen que el hecho de que las computadoras portátiles tengan números de serie hace que sea más difícil comercializar estos objetos hurtados. Sin embargo, esta idea está muy lejana de la realidad, sobre todo en un país como el nuestro, donde no existen registros ni entidades que controlen o den a conocer los listados de los números de serie de las computadoras que han sido robadas.

Incluso, son muchas las personas que, inocentemente, buscan comprar equipos portátiles de segunda mano con la intención de ahorrar costos. En estos casos, las casas de venta a las que se dirigirán son centros independientes de reparación que también venden equipos usados, o cadenas de tiendas que se dedican a la compra y venta de equipos usados y remodelados.

En esencia, hay un gran mercado para el negocio de lo usado, el cual suele ser incluso más amplio para artículos que rápidamente evolucionan, como el caso de las computadoras, teléfonos y computadoras de mano, en el cual existe un extendido tráfico de productos usados y en donde, por ende, existe una mayor facilidad para colocar aquellos artículos que han sido robados.

"Las personas jamás dejarían una bolsa con US$3000 en el carro, en la habitación del hotel o en la maleta en el avión o autobús. Entonces, la pregunta sería por qué dejan su computadora personal en el asiento del acompañante del auto o en el escritorio del hotel y los dejan sin vigilancia" comenta Gustavo Garita, agente del Organismo de Investigación Judicial.

Si se utiliza y se depende de la computadora para las clases de la universidad o para el trabajo, el hecho de que fuese hurtada sería verdaderamente un desastre. Al parecer y según las estadísticas que veremos a continuación, esta situación sucede más a menudo de lo que muchos imaginan.

Estadísticas actuales de robo

En nuestro país, la oficina de estadística del Organismo de Investigación Judicial (OIJ) registra el robo de computadoras y equipo portátil en general como hurto, por lo cual no mantiene un registro de las denuncias que son presentadas anualmente ante la entidad.

Específicamente en el caso de los teléfonos celulares, un estudio publicado en el periódico La Nación el 2 de febrero de 2006 indica que "en nuestro país entre enero y noviembre del 2005 fueron robados 102.000 teléfonos celulares, lo cual equivale al 10% del total de líneas concedidas, que el pasado 14 de enero eran 1.145.000".

El Instituto Nacional de Seguros (INS) mantiene un registro de los reclamos reportados como correctos para el seguro de equipo electrónico; sin embargo, no fue posible obtener un detalle de las categorías por las cuales se efectuaron dichos reclamos, el dispositivo que era cubierto por la póliza, ni tampoco cuántos reclamos no fueron aceptados por la entidad.

Según la tabla 1, en los últimos 5 años, el INS registró 373 reclamos, los cuales representan un total de ¢14.724.904.827 según el monto asegurado en esas pólizas, pero pagó únicamente ¢172.133.722, lo que equivale al 1.16% del total asegurado.

Cuadro #1
INSTITUTO NACIONAL DE SEGUROS
DIVISIÓN DE SEGUROS GENERALES
Número de reclamos aceptados por el INS entre el año 2000 y el 2005

AÑO DE SINIESTRO	MONTO ASEGURADO	MONTO PAGADO	NUMERO DE RECLAMOS	MONTO PAGADO PROMEDIO	MONTO ASEGURADO PROMEDIO
2000	1.655.216.571	29.729.127	74	401.745	22.367.792
2001	2.576.090.712	18.832.908	55	342.417	46.838.013
2002	6.701.912.251	25.852.672	50	517.053	134.038.245
2003	1.604.791.451	29.370.524	41	716.354	39.141.255
2004	1.208.796.360	26.136.907	59	442.998	20.488.074
2005	978.097.482	42.217.584	94	449.123	10.405.292
TOTAL	**14.724.904.827**	**172.139.722**	**373**	**461.501**	**39.476.957**

FUENTE: Reporte de pago realizado a la cobertura de equipo móvil del seguro de equipo electrónico. INS 2000-2005

Estados Unidos, por medio del Instituto Computacional de Seguridad (CSI, por sus siglas en inglés), es uno de los pocos países que cuentan con estudios serios sobre el índice de los fraudes informáticos que ocurren anualmente en ese país, y dentro de la información que este instituto recolecta se encuentran los robos que existen anualmente de equipo portátil.

En el año 2001, por ejemplo, más de 591.000 computadoras personales portátiles fueron robadas o perdidas, lo cual significó un aumento del 53% sobre las 387.000 que fueron reportadas en el año 2000. El estudio del Instituto señala que para las compañías estadounidenses, estos robos representan en promedio $89.000 en pérdidas anualmente.

Para el dueño de una portátil, esos números generan una probabilidad de 1 en 14 de que esta le sea robada. Según el estudio, esa cantidad de portátiles están valoradas en más de 11,8 billones de dólares, pero afirma a su vez que las personas físicas y jurídicas que tienen aseguradas sus computadoras es ínfima, por lo que los números son en realidad mayores.

Estas cifras son más que lógicas si se comprende que los delincuentes ven el robo de computadoras portátiles como de un alto rendimiento, tomando en cuenta la baja inversión en riesgo en la que incurren, como lo puede ser la sustracción de uno de estos aparatos a un trabajador desprevenido y distraído.

El robo de equipo portátil en las empresas

Cuando a un empleado se le asigna una computadora portátil para el trabajo, generalmente también se le ofrecen disquetes, libros de software y, por supuesto, el número de teléfono del departamento de soporte técnico en caso de que tenga un problema.

Sin embargo, son muy pocas las compañías que proporcionan, además, información adicional destinada a proteger del robo de su propiedad, es decir, estas computadoras portátiles, mientras los empleados las utilizan en sus viajes. Es común que las empresas den por un hecho que sus empleados están enterados de todos los trucos y estafas que los delincuentes utilizan, por lo que no se les da mayor información sobre cómo cuidar estos equipos durante los viajes.

“Es una realidad, nosotros no contamos con un manual de procedimientos, políticas o recomendaciones a las que nuestros empleados puedan acceder para informarse acerca de cómo utilizar o cuidar las portátiles, todo con lo que contamos es con una póliza de seguro en caso de daño o pérdida”, comentó Orlando Soto, gerente general del Grupo Financiero ACOBO.

Otra razón por la que muchas compañías no ponen demasiado énfasis en hacerles estas sugerencias a sus empleados, es porque el robo nunca les ha sucedido a sus trabajadores, sin entender que como ya hemos visto, el robo de computadoras portátiles es uno de los más frecuentes y que las posibilidades de que suceda son realmente muy altas.

Es por ello que se vuelve fundamental capacitar a los empleados en todo tipo de estrategias orientadas a la prevención de robos de computadoras portátiles, proporcionándoles sencillas y efectivas sugerencias de seguridad para cuidar sus equipos, lo cual podría potencialmente ahorrarle a la compañía una innumerable cantidad de problemas.

Sucede como ya se ha mencionado, que si uno de los ordenadores portátiles de la compañía es sustraído, no sólo se estará perdiendo el valor del hardware, que podría ser de hecho lo menos importante, sino también toda la información guardada en este. Lo cierto es que la mayoría de las compañías que asigna ordenadores portátiles a sus empleados, están más concentradas en proporcionar información sobre el uso del equipo, antes que sobre la seguridad, y deja de lado cualquier información sobre la prevención de su robo o bien alguna cerradura para asegurarla mientras está fuera de la oficina.

Sin embargo, los empleados que llevan en sus manos un costoso ordenador portátil tendrán, como resultado de este equipaje, un significativo aumento de sus posibilidades de ser víctimas de un robo, por lo que ellos deben ser capacitados en todos los aspectos referentes a cómo mejorar el cuidado de sus computadoras portátiles junto con la información, a menudo confidencial, que estas contienen.

Seguros disponibles en el mercado costarricence para equipo portátil

En nuestro país, el Instituto Nacional de Seguros (INS) tiene una póliza para el equipo electrónico, el cual es definido según el INS como “aquellos equipos cuyo funcionamiento dependa de uno o varios componentes electrónicos” (INS, 2000). La póliza está dirigida a un mercado muy dinámico y de difícil caracterización. “Esta póliza aplica para ordenadores personales, computadoras de mediana y alta capacidad, fotocopiadoras, centrales telefónicas, teléfonos celulares e incluso equipo médico especializado”, según se detalla en la página del Instituto Nacional de Seguros.

El Instituto le ofrece dos categorías para el aseguramiento del equipo, divididas según las tarifas, la valoración y las coberturas ofrecidas: riesgo nombrado y todo riesgo.

En la póliza de riesgo nombrado, “el Instituto dará protección al Asegurado, Causahabientes o cualquier beneficiario indicado en la póliza, e indemnizará las pérdidas o daños materiales directos, accidentales, inmediatos, súbitos e imprevistos que sufran los bienes descritos en la póliza... siempre y cuando hayan sido incluidos en el contrato de conformidad con lo estipulado en las condiciones particulares” (INS, 2000).

Dentro de la modalidad de riesgo nombrado, el INS cuenta con siete tipos de coberturas, de las cuales las primeras seis aplican para todas las pólizas que mantiene la entidad, y pueden ser incluidas dentro de la póliza a criterio del asegurado.

Básicamente, la cobertura tipo A (Incendios) comprende todos los

siniestros derivados de incendio casual, explosión, corto circuito, variaciones de voltaje, rayo, implosión, humo, hollín y otros que puedan declararse en el momento de firmar la póliza.

El robo está amparado dentro de la cobertura B, mientras que la cobertura C determina los siniestros generados por eventos de la naturaleza, dentro de la que están comprendidos los daños derivados de temblor, terremoto, erupción volcánica y golpe de mar por maremoto, entre otros.

Otros riesgos, como los problemas provocados por la acción del agua o por niveles de humedad anormales, hundimientos o deslizamientos de terreno, quedan amparados bajo la categoría D, denominada Otros Riesgos.

Cobertura E: Equipo móvil.
Cobertura F: Teléfonos celulares.

Por último, la cobertura tipo G, asignada exclusivamente para la póliza de equipo portátil denominada Portadores Externos de Datos, se compromete a "indemnizar al asegurado las pérdidas y/o daños materiales indemnizables bajo las coberturas suscritas, que sufrieron los portadores externos de datos..., incluyendo la información almacenada en éstos, que puede ser directamente procesada en sistemas electrónicos de procesamiento de datos" (INS, S.F.).

Según datos del INS (2000): "Las pólizas de riesgo nombrado están disponibles para casas de habitación, oficinas, comercios, industrias, etc.; haciendo la salvedad de que para las primeras, no se puede otorgar la cobertura "S" de Portadores Externos de Datos". Por otra parte, mediante la póliza de todo riesgo "se cubren las pérdidas o daños materiales de los bienes cubiertos como consecuencia directa de cualquier causa siempre y cuando sea súbita e imprevista, excepto las limitaciones y explosiones que se señalan en la sección de Riesgos Excluidos de las Condiciones Generales" (INS, 2000), detalladas en la sección IV del acuerdo de aseguramiento, de las cuales se comentará más adelante. Esta modalidad también ampara coberturas para el equipo móvil, teléfonos celulares y portadores externos de datos.

Otra limitación importante para las pólizas del tipo Todo Riesgo es que el monto mínimo que se puede asegurar por póliza es de ¢100.000.000 o su equivalente en dólares, lo que la convierte en una póliza que aplica exclusivamente a grandes empresas que mantienen una importante cantidad de equipo portátil como parte de sus activos.

Según todo lo anterior y bajo las tarifas actuales para el aseguramiento de equipo móvil, el

cual paga una tasa del 1,25% y una prima mínima de ¢24.000 más impuesto de ventas, por ejemplo, un equipo valuado en US$2100 (¢1.050.000, al tipo de cambio de ¢500) pagaría una prima anual de ¢33.341, y le regiría un deducible del 25% con un mínimo de ¢20.000 por evento. En el caso de los teléfonos celulares que paga una tasa del 9.47% y una prima mínima de ¢6.000.000 más impuesto de ventas, un celular valorado en ¢195.000, pagaría en este caso una prima anual de ¢20.867.

En caso de presentarse un reclamo amparado bajo el seguro de equipo electrónico, el INS aplica una tasa de depreciación con base en el año de fabricación y mediante un método de línea recta, con el que aplica un criterio de vida útil para los equipos portátiles de 5 años.

En caso de un reporte de un evento que esté cubierto por la póliza, el asegurado debe dar aviso de forma escrita como máximo 5 días hábiles después de la fecha en que ocurrió el incidente y debe indicar lo siguiente:

- La fecha del siniestro
- Número de póliza que lo ampara
- Características del equipo siniestrado
- Causa del evento

A su vez, se tienen 15 días naturales para presentar los requisitos solicitados, los cuales varían según el tipo de evento. Si se presenta daño del equipo, es requerida la personería jurídica (en caso de ser el asegurado una persona jurídica) con menos de un mes de emitida; la factura pro forma de un bien igual al siniestrado, que indique el valor de reposición del equipo; y el informe técnico elaborado por un especialista, el cual debe contener al menos: fecha del siniestro, causa del daño, descripción exacta del equipo revisado, monto de los daños (si el equipo tiene reparación) o en su defecto, indicar si se trata de una pérdida total.

Adicionalmente, en caso de robo del equipo, se requiere una fotocopia de la denuncia presentada ante el Organismo de Investigación Judicial (OIJ) u otra autoridad competente, donde se indique claramente al menos: fecha de la sustracción, descripción exacta del equipo robado y forma en que ocurrió el evento, fotocopia del acta de inspección ocular que realiza el Organismo de Investigación Judicial (OIJ) u otra autoridad competente, o fotocopia de aviso al Instituto Costarricense de Electricidad (ICE), con sello de recibido por parte de esa entidad, en caso de que el bien robado corresponda a uno o varios teléfonos celulares.

El Instituto exige que todos los casos en los que se cuente con una póliza en la categoría o modalidad de Todo Riesgo, debe realizarse una inspección adicional por parte del agente respectivo, al igual que en

todas las pólizas de riesgo nombrado donde el monto asegurado sobrepase los ¢40 millones.

Sobre esta revisión existen algunas cláusulas explícitamente determinadas en la sección IV de las condiciones generales del acuerdo de aseguramiento que se debe firmar con el Instinto. Específicamente, la cláusula número 15 exonera al INS del pago de cualquier indemnización en caso de que la pérdida del equipo quede categorizada por el OIJ bajo el denominativo de "hurto". El Diccionario de la Real Academia (2001) define el hurto como "el delito que consiste en tomar con ánimo de lucro cosas muebles ajenas contra la voluntad de su dueño, sin que concurran las circunstancias que caracterizan el delito de robo", y define el robo como el "delito que se comete apoderándose con ánimo de lucro de una cosa mueble ajena, empleándose violencia o intimidación sobre las personas, o fuerza en las cosas".

En otras palabras, para que la póliza pueda ser reclamada por el afectado deben quedar indicios de violencia para que el OIJ categorice el hecho como robo y no como hurto, siendo este último la forma más frecuente por la cual es perdido el equipo portátil.

Medios comunes para la protección de equipo portátil

Existen en el mercado actual varios métodos para prevenir el robo de equipo portátil, aun cuando los cuidados que cada usuario pueda tener con su equipo siguen siendo las mejores armas contra el hampa en este tipo de delito.

En Estados Unidos, por ejemplo, la compañía SafeRegistry ha definido el robo de equipo portátil como cuestión de etiqueta, pues lo que hace es proveer al propietario un adhesivo que se coloca en la computadora portátil, teléfono celular o cualquier otro artículo que desea proteger, el cual cuenta con un número de localización y sencillas instrucciones sobre cómo devolver el artículo.

El sistema, aunque muy sencillo, funciona, afirma Dan Yost, presidente corporativo de SafeRegistry, quien afirma que la etiqueta hace que el objeto pierda mucho **valor** al ser revendido, ya que anuncia que ha sido robado; además, agrega "La etiqueta es prácticamente imposible de despegar —en una escala de **poder** adhesivo de 1 a 10, cuenta con un 'pegamento 10'— y funciona mejor cuanto más visiblemente se instale en la computadora".

Las etiquetas de SafeRegistry, firma creada por Tri-8, Inc., cuestan entre US$29 y US$49 al año, y se obtienen cuatro por el precio más reducido, de forma que puedan **util**izarse no sólo para la "laptop", sino tam**bién** para otros artículos móviles como el celular, "Ipods", computadoras de mano, cámaras de video o hasta en una bicicleta.

Existen en el mercado otros mecanismos como los candados de seguridad, los cuales permiten amarrar las computadoras portátiles a la zona donde se trabaja; por ejemplo el cable de seguridad de Conceptronic, que previene el robo de equipos portátiles. Este dispositivo es compatible con cualquier portátil que disponga de un anclaje de seguridad que se encuentra en la mayoría de las computadoras portátiles actuales, y simplemente se debe asegurar el cable de 1,90 metros de longitud a un objeto pesado y difícil de mover y acoplarlo a la portátil mediante cualquiera de las llaves suministradas.

Otras soluciones han tratado de ir un poco más allá habilitando opciones remotas de seguridad, como alarmas que se disparan si el equipo portátil se aleja cierta distancia, o detectores de huellas que eliminan la capacidad de acceso a la información contenida en estos dispositivos en caso de hurto.

Sin embargo, este tipo de soluciones puede que amedrenten a un ladrón común; sin embargo, los ladrones profesionales dedicados a este tipo de delito no los consideran un obstáculo.

Según los expertos consultados, existen casos en los que para abrir las cerraduras ha bastado un simple pedazo de cartón debidamente doblado. Por lo demás, la cadena que forma parte de los dispositivos antirrobo tiene poco espesor, por lo que romper o cortar este tipo de candados no resulta complicado.

Los detectores de movimiento tampoco amedrentan al ladrón experimentado, pues estos dispositivos reaccionan sólo después de un momento, señala el experto. El ladrón tiene así suficiente tiempo para escapar en una dirección mientras deja el detector de movimiento tirado en otro lugar para distraer a la víctima, o la alarma puede incluso pasar inadvertida en medio del bullicio de una feria o de un ruidoso entorno. Para ello hay que asegurarse de que la cadena del candado sea estable y esté ubicada en una parte importante de la caja de la “laptop”. De lo contrario, el ladrón simplemente la arrancará.

A nivel corporativo existen soluciones para empresas que se encuentran muy expuestas a este tipo de crimen; por ejemplo, el sistema antirrobo Asset Sentry de la empresa estadounidense CISCOR previene el robo de equipo portátil por parte de los empleados o cualquier otra persona registrando los movimientos de material dentro de la compañía. De esta manera y mediante sensores completamente automáticos, el sistema de CISCOR registra si cualquier parte del dispositivo monitoreado es alterado, sustraído o desconectado, activando inmediatamente una alarma en una computadora central, la cual se encarga de difundir el evento

mediante las opciones que tenga programadas como radios portátiles de mano, fax, teléfono, altavoces instalados en la empresa o correo electrónico, de esta forma completamente automatizada se minimiza el error humano y se asegura una respuesta más rápida y segura ante cada evento registrado.

Recuperación de equipo portátil a través de internet

La afición o la necesidad hacen que muchas personas no se desconecten de internet en sus vacaciones y recurran a la red allá donde van para consultar el correo, escribir en su página web o, simplemente, navegar. Entre estos últimos también hay dos tipos de veraneantes: los que no olvidan colocar en el equipaje la computadora portátil, la PDA y todo lo necesario para conectarse a internet; y quienes confían en encontrar en su destino un lugar de acceso público, bien sea un "cibercafé", un locutorio o desde el propio hotel.

Desde que salió la versión profesional del programa Computrace a mediados del año 2001, no sólo los carros están protegidos por satélites, sino que también los objetos personales y de oficina cuentan con una protección similar. Programas de este tipo actúan como un radiofaro que, en caso de que el ordenador sea robado, indican de forma invisible para el ladrón, la posición del equipo cada vez que este se conecta a internet.

Fue la empresa estadounidense Gateway la que comenzó a incluir en sus computadoras portátiles y "notebooks" un dispositivo antirrobo. La solución permite que los equipos de Gateway puedan avisar en qué lugar se encuentran en caso de ser perdidos o robados por los eternos amigos de lo ajeno.

Actualmente otros fabricantes como IBM, Dell y Sony han incorporado esta tecnología a sus modelos. Sin embargo, en el caso de computadoras de otras marcas, los creadores de Computrace han hecho alianzas con empresas de seguridad, una de las cuales es Lo Jack for Laptops, quienes se han aventurado en el mercado de la recuperación de equipos portátiles con muy buenos resultados.

El programa consiste en un agente encargado de impulsar el servicio ComputracePlus, silencioso e invisible y que no puede ser detectado mirando en el directorio o al ejecutar una herramienta que examine la memoria RAM. Absolute, la empresa que cuenta con la patente de este programa, ha probado con éxito ComputracePlus utilizando los mayores paquetes de detección de virus sin que haya sido detectado.

El agente de Computrace es una utilidad de bajo nivel resistente a las alteraciones, igual que lo puede ser una utilidad basada en disco. El agente no se puede eliminar del disco duro al borrar los archivos, porque no está visible en los directorios de los

archivos, inclusive puede resistir formateos del disco duro, comandos del disco F y particiones del disco duro, únicamente un agente autorizado con la contraseña y el software de instalación correcto puede eliminar el agente.

Cuando un ordenador reportado como robado se conecta a internet, el sistema Computrace envía una señal silenciosa al Centro de Monitorización de Absolute cada 15 minutos, incluyendo en ella la dirección IP o el número de teléfono del sitio por donde se está accediendo a internet, y esta información es suministrada a las autoridades competentes quienes se encargan de recuperar la portátil.

Para que el sistema sea operable, básicamente la computadora debe contar con un procesador 486 o superior, un MODEM compatible con Hayes o conexión a internet y contar con Windows 95/98/2000/NT/Me/XP como sistema operativo, lo cual lo hace operable en prácticamente cualquier PC.

Otra de las características del sistema es que toda la información confidencial que contenga la computadora robada, puede ser borrada en forma remota. De esta manera se protegen los datos que podrían ser riesgosos en manos de terceros.

Según el sitio en internet de Lo Jack for Laptops, el 90% de las computadoras portátiles protegidas por este sistema son recuperadas y para hacer aún más tentadora la oferta de este sistema de protección, las empresas asociadas se comprometen a encontrar los equipos dentro de los 60 días siguientes o a reembolsar el valor de este.

En el caso de las computadoras portátiles de Apple, se ha desarrollado un software con características similares llamado Undercover. El servicio funciona básicamente de la misma forma aunque un tanto más primitiva, ya que este software fue desarrollado por un belga llamado Peter Schols y no cuenta con el respaldo de Apple.

Primero, se debe instalar el software e inscribirlo en el servidor de Orbicule; en el momento en que la computadora Mac es robada, el usuario debe reportarla como tal en el servidor para que la localización inicie, de esta forma la próxima vez que la persona que tiene el equipo se conecte a internet (Ethernet, WiFi, Bluetooth, FireWire, etc.), el sistema envía “pantallazos" de las aplicaciones que están utilizando. Si eso no ayuda con la localización, desde el servidor se puede activar un "Plan B", el cual consiste en que la Mac muestre un mensaje de error falso que indica que hay problemas serios de hardware y no se puede utilizar.

La idea detrás de todo esto es que cuando lleven la Mac a un servicio técnico, se darían cuenta de que es

un error falso y al salir de él aparezca un mensaje alertando al servicio técnico con respecto a que este Mac ha sido robado, junto con información de contacto y quizás una recompensa.

Está claro que este segundo sistema es mucho menos confiable que el desarrollado para las PC, pero por lo menos es un intento por ofrecer una opción a los usuarios de computadoras de Apple.

Consejos para minimizar el impacto del robo

En nuestros días, el uso de dispositivos portátiles no se limita únicamente a usuarios de negocios que viajan constantemente; gracias al avance que ha tenido la tecnología, estos equipos se han convertido en una constante en la vida común de las personas y mientras ese avance tecnológico las hace más populares y convenientes, también los hacen un blanco ideal para los ladrones. Es por ello importante tomar algunas medidas tanto para minimizar la exposición al robo, como para disminuir el impacto por la pérdida de la información.

Recae, no obstante, sobre cada individuo la responsabilidad de determinar el nivel de riesgo bajo el que se encuentra actualmente. En caso de robo, la más obvia pérdida es la máquina en sí; sin embargo, si el ladrón puede acceder a la información contenida en el dispositivo, también la información está en riesgo, así como cualquier otra información que sea accesible a través de los datos ahí almacenados.

La información corporativa significativa o la información de cuentas de clientes no deben ser accedidas por personas no autorizadas. Constantemente es posible escuchar noticias acerca de portátiles perdidas o robadas con información confidencial o valiosa. Sin embargo, aun si no hay ninguna información corporativa importante en ellos, cada uno de estos aparatos contiene información valiosa como: las citas de su agenda, claves, direcciones de correo electrónico, información de contactos, información personal de cuentas en línea, por solo citar algunas.

Proteja su información

Existen pasos básicos que todo usuario de dispositivos portátiles debería poner en práctica, independientemente del equipo portátil que utilice. Cada funcionario debe estar al tanto del valor del ordenador portátil y de las razones por las cuales es tan importante protegerlo del robo, sea propiedad personal o de la empresa.

Algunas compañías podrían ofrecer a sus empleados un seguro que cubra el robo de sus ordenadores portátiles, pero en cualquier caso se deberá proveer a sus trabajadores un dispositivo de seguridad para asegurar el ordenador portátil tanto en los viajes como incluso dentro de

la oficina, pues más del 40% de todos robos de ordenadores portátiles se realiza en las oficinas.

Específicamente, es necesario estar enterados de las ubicaciones más riesgosas y de los métodos de los ladrones para hurtar ordenadores portátiles, pues una actitud proactiva de seguridad puede ahorrar miles de dólares, incluyendo los potenciales juicios a empleados que fingen ser víctimas del robo de los datos de clientes, que de hecho pueden haber vendido a la competencia.

A continuación se enumeran algunas recomendaciones generales.

1. No perder de vista el ordenador portátil.
La mayoría de los robos de ordenadores portátiles ocurren en hoteles, aeropuertos o mientras se está alquilando un auto. Los delincuentes no necesitan un arma para robar un ordenador portátil, simplemente esperan que sus dueños se distraigan cuando, por ejemplo, hagan una llamada en la cabina telefónica del aeropuerto.

Por eso, si debe hacer cualquier tipo de acción, cerciórese de que la computadora esté directamente frente a usted, no a la izquierda, derecha, ni detrás, pues un ladrón puede durar menos de cinco segundos en arrebatar el equipo.

2. Mantener el ordenador portátil con cierre de seguridad

Si se debe salir fuera de un hotel, seguramente no se dejaría una cartera sin candado con efectivo u objetos de valor dentro de la habitación, entonces, ¿por qué sí se dejaría un ordenador portátil?

Lo cierto es que no debe dejar uno de estos equipos solo en un cuarto de hotel, sin asegurarlo previamente con un dispositivo que lo fije a un escritorio o, por lo menos, con una cerradura de cable o con una conexión a un cable de alarma escondido, y siempre en un espacio seguro. Se debe recordar que los delincuentes profesionales son grandes actores y actrices, que pueden ingresar en los cuartos mientras el servicio doméstico hace el mantenimiento, diciendo que ese es su cuarto.

Se debe ser también muy cuidadoso con respecto a dejar el ordenador portátil en los espacios de conferencia del hotel, pues existen numerosos robos que ocurren cuando los dueños dejan sus equipos por apenas cinco minutos durante un recreo en la reunión, ya que nadie verifica la identificación de las personas que entran y salen de la sala de conferencia, y menos durante los recesos.

3. Sugerencias de ubicación y control del ordenador portátil
Aunque el robo de una computadora personal portátil puede ocurrir en cualquier lugar o momento, existen ciertas ubicaciones más vulnerables

tanto en las oficinas como en los aeropuertos, hoteles, centros de conferencias, universidades, bibliotecas y hospitales, en las cuales normalmente se producen estos robos.

Por eso, sería muy importante prestar una particular atención a los equipos cuando estén en estas ubicaciones. En los lugares como hospitales y bibliotecas, los ordenadores portátiles son hurtados por gente que aparenta tener una razón legítima para estar allí. Esto puede incluir al público asistente, el personal de limpieza, los contratistas, los custodios, el personal de atención o incluso vendedores.

En este sentido, es importante recordar que no se deben dejar ordenadores portátiles desatendidos, especialmente en la noche o en las mesas de las salas de conferencia. Si el escritorio está en un área de alto tráfico o un área accesible al público en general, se debe fijar el ordenador portátil en cualquier momento en el que usted esté lejos del escritorio.

Asimismo, no se deben dejar ordenadores portátiles cerca de ventanas exteriores, donde sean susceptibles a golpes o arrebatos.

4. Cuidado del ordenador portátil dentro del auto
Si un ordenador portátil se debe dejar dentro de un auto, mantenga el carro cerrado y el equipo fuera de la vista (por ejemplo, dejándolo debajo de un asiento).

Mientras conduce, coloque el equipo en el asiento del acompañante, y mantenga la ventana y la puerta debidamente cerradas ya estos equipos pueden ser sustraídos en un congestionamiento.

5. Traslado del ordenador portátil
Si lleva el equipo en un portafolio diseñado especialmente para computadoras portátiles, los ladrones estarán inmediatamente alertas de que posee uno de estos equipos, incluso antes de que lo saque para comenzar a trabajar. Por eso, llevar su ordenador portátil en un equipaje o cartera ordinario lo ayudará a disuadirlos de su robo.

6. Proteja el equipo con una palabra de paso segura
Asegúrese de que deba ingresar una contraseña segura para conectarse a su equipo portátil; esta contraseña debe ser como mínimo de ocho caracteres, incluida una combinación de letras, números y símbolos que sea fácil de recordar, pero difícil de adivinar por terceros. Muchas computadoras personales en la actualidad tienen incorporados dispositivos biométricos para asegurar que la información es accedida por la persona correcta.

7. Mantenga un respaldo actualizado de los archivos
Si el equipo es robado, ya es lo suficientemente malo que un tercero tenga acceso a su información. Para evitar perder toda la información, es

recomendable realizar respaldos de la información importante y guardarlos en lugares separados, de esta manera no solo se está en condiciones de recuperar la información perdida, sino que además se es capaz de identificar y reportar exactamente la información que está en peligro.

Los empleados que viajen con ordenadores portátiles que tengan una información importante para la empresa, deben utilizar discos rígidos desmontables y llevarlos separadamente de sus ordenadores portátiles.

8. "Encripte" la información que almacena en el dispositivo portátil
De esta manera se asegura que la persona que sustrajo el equipo no podrá tener acceso a la información que tenía almacenada. Un ejemplo es el sistema EFS, que ofrece la posibilidad de "encriptar" archivos y carpetas por medio de este sistema; así, si alguien no autorizado consigue obtener acceso a un archivo después de sustraer, por ejemplo, una computadora portátil o un disco, no podrá "desencriptar" el archivo y ver su información.

El sistema EFS incorpora varias capas de cifrado para incrementar la seguridad, cada archivo cuenta con una clave de cifrado de archivo única, indispensable para poder "desencriptar" los datos del archivo. Esta clave, que también está cifrada, sólo está en posesión de los usuarios que tienen autorización para ver los datos. EL EFS está integrado en el sistema de archivos, lo que dificulta aún más cualquier acceso no autorizado y, al mismo tiempo, facilita la administración por parte de los usuarios.

El proceso de cifrado y descifrado de datos es totalmente transparente y prácticamente no requiere intervención por parte del usuario, que sólo debe elegir el archivo que desea "encriptar".

Recomendaciones adicionales para las empresas
Cree una atmósfera donde los empleados se actualicen regularmente sobre las nuevas metodologías de robos, sustracciones y estafas de ordenadores portátiles. Esto puede ser logrado realizando seminarios de prevención y utilizando medios de información como boletines y sistemas de correo electrónico internos.

Establezca una política que haga a los empleados responsables de la pérdida de sus ordenadores portátiles, si es que ellos no siguen al pie de la letra la política de la compañía para prevenir las sustracciones de estos equipos cuando estén fuera del edificio de la empresa. Comunique esta política por escrito y obtenga una declaración firmada de su conocimiento por parte de los empleados.

Mantenga un inventario de todos los ordenadores portátiles y

computadoras poseídas por la compañía. Sepa dónde y a quiénes fueron asignadas. Mantenga un registro de los números de serie, inclusive de los que correspondan a los discos rígidos.

Todos los ordenadores portátiles deben ser grabados o marcados permanentemente para que puedan, mediante este recurso, ser más fáciles de recuperar si son encontrados por la policía. Consulte al fabricante con respecto a los criterios apropiados sobre lugares para marcar y garantías antes de marcarlos o grabarlos.

Siguiendo estos simples pero efectivos consejos es posible agregar un grado más de protección a la información que comúnmente es almacenada en equipos portátiles. Sin embargo, los expertos enfatizan que las soluciones no tecnológicas son las más importantes de seguir y que una atención preactiva del problema por parte de cada uno de los usuarios de equipo portátil, estando siempre alerta, son los mejores caminos para enfrentar este creciente problema.

BILIOGRAFÍA

CISCOR. (2006). Sistema de rastreo de equipos de valor y dispositivos antirrobo. Recuperado el 16 de marzo de 2006, de http://www.ciscor.com/es/sistemas/sistema_de_rastreo_de_bienes_equipos_de_valor_y_dispositivos_antirobo.html

Dell. (2006). CompuTrace Plus. Recuperado el 16 de marzo de 2006, de http://www1.euro.dell.com/content/learnmore/learnmore.aspx/computraceplus?c=es&cs=esbsdt1&l=es&ref=CFG&s=bsd&~lt=popup&~tab=1

Instituto Nacional de Seguros. (2000). *Manual tarifario y políticas de aseguramiento. Equipo Electrónico*. Costa Rica: Instituto Nacional de Seguros.

Instituto Nacional de Seguros. (S.F.). *Seguro de equipo electrónico riesgo nombrado. Condiciones Generales*. Costa Rica: Instituto Nacional de Seguros.

Instituto Nacional de Seguros. (2006). Seguro de Equipo Electrónico. Recuperado el 2 de febrero de 2006, de http://portal.ins-cr.com/Empresas/SegurosCo/equipoElectronicoEm/

Safe Registry. (2006). Recuperado el 12 de febrero de 2006, de http://saferegistry.com