SUPRESIÓN ELECTRÓNICA DE VENTAS: UNA AMENAZA PARA LOS INGRESOS FISCALES

OCDE

ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICOS

La OCDE constituye un foro único en su género, donde los gobiernos trabajan conjuntamente para afrontar los retos económicos, sociales y medioambientales que plantea la globalización. La OCDE está a la vanguardia de los esfuerzos emprendidos para ayudar a los gobiernos a entender y responder a los cambios y preocupaciones del mundo actual, como el gobierno corporativo, la economía de la información y los retos que genera el envejecimiento de la población. La Organización ofrece a los gobiernos un marco en el que pueden comparar sus experiencias políticas, buscar respuestas a problemas comunes, identificar buenas prácticas y trabajar en la coordinación de políticas nacionales e internacionales.

Los países miembros de la OCDE son: Alemania, Australia, Austria, Bélgica, Canadá, Chile, Corea, Dinamarca, Eslovenia, España, Estados Unidos de América, Estonia, Finlandia, Francia, Grecia, Hungría, Irlanda, Islandia, Israel, Italia, Japón, Luxemburgo, México, Noruega, Nueva Zelanda, Países Bajos, Polonia, Portugal, Reino Unido, República Checa, República Eslovaca, Suecia, Suiza y Turquía. La Unión Europea participa en el trabajo de la OCDE.

Créditos de las fotografías: cover photo © Patryk Kosmider - Fotolia.com

Índice

Resumen

Las técnicas de "supresión electrónica de ventas" facilitan la evasión fiscal y tienen como consecuencia enormes pérdidas fiscales a nivel mundial. Los sistemas de punto de venta (POS) en el sector minorista son un elemento fundamental de todos los sistemas de ventas y contabilidad y una herramienta fiable para la contabilidad y la gestión de una empresa. Por consiguiente, se espera que contengan los datos originales que los auditores fiscales deberán inspeccionar. En realidad estos sistemas no sólo permiten "capturar" (skimming) los recibos de cobro tal como los sistemas manuales, a saber, las cajas registradoras, sino que una vez dotados de un software de supresión electrónica de ventas, facilitan fraudes mucho más elaborados gracias a su capacidad de recrear registros que correspondan a la captura de transacciones.

Las administraciones tributarias están perdiendo miles de millones de dólares y euros debido a las ventas no declaradas y a los ingresos ocultados mediante la utilización de estos métodos. Según una asociación canadiense de restauradores, la supresión de ventas en los restaurantes en ese país asciende a cerca de 2.400 millones de dólares canadienses al año. Desde que el Grupo de Trabajo de la OCDE sobre Delitos Fiscales y otros Delitos empezó su labor y a concienciar acerca de este fenómeno, varios países (incluidos Francia, Irlanda, Noruega y el Reino Unido) han examinado sus sectores minoristas y han descubierto importantes problemas. Entre estos países, Irlanda ha reaccionado con prontitud para poner en práctica una legislación que contribuya a combatir los abusos. Asimismo, varios países consideran que abordar esta cuestión de manera agresiva forma parte importante de una estrategia para reducir la brecha fiscal general.

En este informe se describen las funciones de los sistemas de punto de venta y las áreas de riesgo específicas. También se exponen en detalle las técnicas de supresión electrónica de ventas que los expertos han identificado, en particular la utilización de programas “Phantomware” y “Zapper”, y se explica cómo los auditores e investigadores fiscales pueden detectar dichas actividades. También se señala el constante desarrollo de las técnicas de supresión electrónica y la necesidad de estar atento a los cambios.

En el informe se recopilan y analizan las respuestas que los gobiernos han puesto en práctica para combatir los abusos derivados de la supresión electrónica de ventas y se identifican algunas de las mejores prácticas. Entre éstas se encuentran el refuerzo del cumplimiento de las normas haciendo hincapié en el cumplimiento voluntario mediante la intervención de organizaciones profesionales, la concienciación de todas las partes interesadas, incluido el público en general, el mejoramiento de las habilidades de auditoría e investigación, la recopilación y el intercambio de informaciones y la aplicación de soluciones técnicas tales como la implantación de sistemas de punto de venta certificados.

En el informe se hacen las siguientes recomendaciones:

- Las administraciones tributarias deben desarrollar una estrategia para abordar la cuestión de la supresión electrónica de ventas dentro del enfoque general del cumplimiento de las obligaciones fiscales teniendo en cuenta los riegos provocados por los sistemas de supresión electrónica de ventas, promover el cumplimiento voluntario de las normas y mejorar los métodos de detección y la aplicación de contramedidas.
- Las administraciones tributarias deben desarrollar un programa de comunicación con el objetivo de concienciar a todas las partes interesadas acerca de la naturaleza criminal de la utilización de este tipo de técnicas y de las graves consecuencias de investigación y procesamiento judicial.
- Las administraciones tributarias deben examinar si su poder jurídico se adapta a las necesidades de auditoría y peritaje de los sistemas de punto de venta.
- Asimismo deben invertir para capacitarse y adquirir las herramientas para realizar las auditorías e investigaciones de los sistemas de punto de venta, lo que incluye determinar el papel de los especialistas en ciberaudoría y contratar expertos para el peritaje de sistemas digitales siempre que proceda.
- Las administraciones deben considerar la posibilidad de recomendar la creación de leyes para penalizar el suministro, la posesión y la utilización de software de supresión electrónica de ventas.

Introducción

Antecedentes

La utilización de técnicas de supresión electrónica de ventas en los sistemas de punto de venta es una evolución inquietante de la evasión fiscal que ha venido desarrollándose durante más de un decenio. Durante ese tiempo, los intentos para afrontar este fenómeno se han concentrado principalmente en Canadá, Alemania, Países Bajos y Suecia. Desde que el Grupo de Trabajo de la OCDE sobre Delitos Fiscales y otros Delitos empezó a trabajar sobre el tema y a concienciar acerca de este problema, otros países (incluidos Francia, Irlanda, Noruega y el Reino Unido) han decidido tomar cartas en el asunto. El objetivo de este informe es divulgar más ampliamente esta práctica, mostrar que solucionar este problema requiere una amplia gama de soluciones técnicas y operativas, pero también de política y estrategia, y hacer recomendaciones que los gobiernos y las administraciones tributarias puedan poner en práctica.

Las cajas registradoras modernas utilizadas en el sector minorista, con frecuencia dotadas de un software empresarial estándar, funcionan como un sistema global de ventas y contabilidad que sirve de herramienta fiable para la contabilidad y la gestión de una empresa. Por consiguiente, se espera que contengan los datos originales que los auditores fiscales deben inspeccionar, incluidos los datos sobre el impuesto al valor agregado (IVA) o el impuesto sobre las ventas. Parece ser que actualmente estos sistemas pueden manipularse para poder "capturar" (skimming) los recibos de cobro tal como lo permiten los sistemas manuales (cajas registradoras o sistemas de doble caja), pero una vez dotados de un software de supresión electrónica de ventas, facilitan fraudes mucho más elaborados gracias a su capacidad de recrear registros correspondientes a la captura de transacciones.

Los términos caja registradora electrónica (ECR) o sistema electrónico de punto de venta (EPoS) se utilizan con frecuencia para describir las cajas registradoras modernas, pero en este informe ambos términos o sus híbridos se denominan bajo el término genérico de "sistemas POS".

El presente informe ha sido elaborado con la colaboración de peritos, ciberauditores e investigadores fiscales, así como de responsables de políticas[1], quienes además han desarrollado un conjunto de herramientas (que incluye paquetes de formación, orientación y una biblioteca con información técnica) destinado a investigadores y auditores fiscales. Gracias a esta experiencia han logrado avances en su trabajo y las herramientas que han creado serán de gran ayuda para otras administraciones tributarias.

En el informe se estudian las funciones de las cajas registradoras modernas y se analiza el papel que desempeñan los fabricantes, los proveedores y los demás actores que participan en su utilización. Se examinan las diferentes herramientas y técnicas de supresión de ventas identificadas, así como los indicios forenses que pueden conducir a su descubrimiento. Asimismo se analizan las estimaciones disponibles sobre la

propagación de la práctica y las pérdidas fiscales resultantes, se describen distintas estrategias de investigación y disposiciones para garantizar la observancia de las normas que los países pueden adoptar y se hacen recomendaciones sobre las medidas que se pueden implementar.

Otros trabajos relacionados

En este informe se analiza principalmente el comportamiento criminal que supone la supresión electrónica de ventas, así como la labor de los investigadores para detectar, erradicar y perseguir este tipo de comportamiento. El Programa Fiscalis de la Unión Europea y el Foro de la OCDE sobre la Administración Tributaria han realizado otros trabajos más orientados hacia el cumplimiento de las normas y las situaciones que afrontan los auditores.

En 2006, el **"Grupo de Proyecto sobre Cajas Registradoras"[2] de la Unión Europea**, en el marco del Programa Fiscalis, realizó una "Guía de Buenas Prácticas en materia de Cajas Registradoras"[3], la cual incluye una revisión general de la legislación de todos los Estados Miembros de la UE, los sistemas de hardware y software para cajas registradoras disponibles, un catálogo de riesgos específicos y recomendaciones sobre mejores prácticas para la auditoría de cajas registradoras y sistemas POS.

Por su parte, el **Foro sobre la Administración Tributaria** emitió en abril de 2010, una Nota de Orientación que incluye recomendaciones sobre los procedimientos para garantizar la fiabilidad de los registros electrónicos[4].

En la segunda mitad de 2010, en el marco del **Grupo de Proyecto de la UE sobre ciberauditoría**, se estableció un Equipo de Actividades sobre los programas Zappers y Phantomware (ZAPAT). Con base en la evolución y las nuevas soluciones de auditoría adoptadas por las administraciones tributarias de los Estados Miembros de la EU, ZAPAT reunirá las mejores prácticas para mejorar la auditoría de los sistemas POS. Con base en sus hallazgos, el Equipo de Actividades producirá una Nota de Orientación sobre la ciberauditoría de los sistemas POS, la cual estará a disposición de los auditores en los países miembros de la UE y completará el trabajo presentado en este informe.

Estimación de las pérdidas fiscales y otros fraudes

La Asociación Canadiense de Restaurantes y Servicios Alimentarios calculó que las ventas suprimidas en 2009 en el sector de la restauración podrían avecinar los **2.400 millones de dólares canadienses**

Se calcula que en Québec, las pérdidas fiscales entre 2007 y 2008 fueron de **417 millones de dólares canadienses**

Suecia recuperó **150 millones de euros** gracias a 2.000 auditorías realizadas durante 4 años

En Sudáfrica se expatriaron **22 millones de euros** en un solo caso

En Noruega, un único caso involucró **7 millones de euros** no declarados

El cálculo de las pérdidas debidas a la supresión electrónica de ventas se ha hecho con respecto a sectores determinados y a regiones geográficas específicas, y son indicio de posibles pérdidas en otras regiones. En Canadá existen valiosas estadísticas basadas en pruebas concretas obtenidas en los casos descubiertos. El Ministerio de Hacienda de

Québec, encargado de la administración y recaudación de los impuestos sobre la renta y al consumo en esta provincia, estimó que entre 2007 y 2008 las pérdidas fiscales por dichas prácticas se elevan a 417 millones de dólares canadienses.

En 2008, la Agencia Canadiense de Ingresos acusó a los propietarios de 4 restaurantes de evasión por "omisión" (zapping) en cerca de 200.000 transacciones por un valor de 4,6 millones de dólares canadienses. La Asociación Canadiense de Restaurantes y Servicios Alimentarios calculó que en 2009 las ventas en efectivo "fantasma" (phantom) podrían avecinar los 2.400 millones de dólares canadienses.

En el Informe Anual sobre la Gestión Financiera Federal de 2003, el Tribunal Federal de Cuentas de Alemania (Bundesrechnungshof), expresó su preocupación por las pérdidas debidas a la supresión electrónica de ventas y concluyó que "con transacciones en efectivo por un valor de miles de millones de euros, el riesgo de evasión fiscal no debe subestimarse[5]".

Otros indicadores son:

- En un caso investigado en Noruega se encontró una suma equivalente a 7 millones de euros no declarados
- En un caso en Sudáfrica, los mayoristas habían expatriado una suma equivalente a 22 millones de euros
- En una investigación realizada en Eslovenia, los inspectores hicieron indagaciones en tiendas minoristas al final de la jornada comercial y descubrieron que en ese momento el volumen de ventas en los sistemas era tres veces superior al registrado otros días.

El Organismo Tributario de Suecia ha abordado la cuestión en el contexto de la brecha fiscal nacional. Según sus estimaciones, el volumen de negocios total de todas las empresas que manejan efectivo en este país es de 100.000 millones de euros. La brecha fiscal calculada de las empresas que manejan efectivo es de 2.000 millones de euros, lo que corresponde a 1/6 del total de la brecha fiscal.

Entre 2006 y 2010, Suecia llevó a cabo cerca de 2.000 auditorías en restaurantes, salones de belleza, tiendas de ropa y tiendas de alimentos, entre otros comercios. El pago incompleto de impuestos en las empresas auditadas fue aproximadamente de 150 millones de euros entre impuestos sobre la renta, IVA y contribuciones empresariales. Las auditorías mostraron que entre el 20% y el 40% del volumen de negocios no se declaraba. Esta omisión está alimentando el mercado gris y la economía subterránea y en algunos casos sustenta el crimen organizado.

Existen pruebas de que la utilización de programas “Phantomware” y “Zapper” se ha extendido en todo el mundo, y por lo tanto la amenaza sobre la recaudación de ingresos tributarios sigue creciendo. Algunos proveedores de software para sistemas POS de restaurantes, por ejemplo, proponen funciones que permiten la supresión electrónica de ventas a nivel internacional. Según las previsiones de los auditores e investigadores que trabajan en el ámbito, en el futuro las técnicas para evitar la detección seguirán desarrollándose y su sofisticación será cada vez mayor.

Por el momento no hay indicios de empresas que recurran a técnicas similares para inflar las ventas, por ejemplo, para lavar dinero de origen criminal. Sin embargo, es una posibilidad y las administraciones tributarias deben ser conscientes de este riesgo.

Notas

1. El Grupo de expertos estuvo coordinado por Noruega y contó con la participación de Alemania, Bélgica, Canadá, Estados Unidos, Francia, Grecia, Irlanda, Noruega, Países Bajos, Portugal, Reino Unido, Suecia y Turquía.

2. El objetivo del Grupo de Proyecto es identificar los riesgos que suponen las cajas registradoras y los sistemas POS, y proponer ideas para contrarrestarlos. Los objetivos detallados de este Grupo de Proyecto fueron:
   - recopilar las diferentes reglas y exigencias presentadas por las autoridades de los Estados Miembros de la UE sobre las cajas registradoras y los sistemas POS, así como la manera en que se utilizan en realidad, a saber, un inventario de las reglas y condiciones para la industria del hardware y software;
   - recoger, compartir y mejorar el conocimiento y la experiencia de las características técnicas de las cajas registradoras y los sistemas POS;
   - determinar distintos conceptos e intercambiar experiencias para mejorar la utilización de los datos sobre transacciones comerciales en las auditorías fiscales; y
   - reunir información sobre cómo los diferentes sistemas pueden utilizarse de manera abusiva.

3. *Cash Register Good Practice Guide*, Grupo de Proyecto del Programa Fiscalis de la UE 12, 2006. (No disponible al público).

4. *Guidance and Specifications for Tax Compliance of Business and Accounting Software*, Foro sobre la Administración Tributaria, OCDE, abril de 2010.

5. Circular del Parlamento Federal de Alemania 15/2020 en 197-198 (nov. 24 de 2003).

Sistemas de Punto de Venta

Sistemas POS

Cuando James Ritty inventó la primera caja registradora en 1879, su objetivo era crear un sistema para registrar las transacciones en efectivo con el fin de evitar que los empleados de su establecimiento robaran sus ganancias. Uno de los primeros modelos se promocionó como el "cajero incorruptible", y pronto se convirtió en la herramienta principal para gestionar las finanzas de todo negocio. El registro preciso de las transacciones de venta y su conservación siguen siendo uno de los principales requisitos de las cajas registradoras. Los recibos que emiten sirven de documento de venta entre los clientes y la empresa. Así, el recibo de la caja registradora es el primer documento o declaración que describe la transacción. Con el tiempo, la función de la caja registradora ha evolucionado, no sólo en cuanto a la documentación de las transacciones de venta, sino a los requisitos de contabilidad y auditoría.

La evolución ha continuado y los negocios ahora utilizan modernos sistemas POS por muchas razones. Ofrecen seguridad y control del dinero en efectivo, son rápidos, disminuyen la cantidad de errores en las transacciones, facilitan la contabilidad y la elaboración de informes, permiten el control de las reservas, ayudan al seguimiento del trabajo de los empleados, emiten recibos y generalmente contribuyen a la imagen profesional de los negocios.

En los sectores minoristas, hotelero y de restauración, las cajas registradoras desempeñan un papel importante en el proceso de gestión. La introducción de la transacción o el pedido del cliente desencadena las acciones subsiguientes, así por ejemplo, el pedido en un restaurante puede transmitirse automáticamente a la cocina, al mismo tiempo que la atención del cliente se asigna a un camarero determinado. En los sistemas de negocios completamente integrados, si bien el sistema POS es sólo uno de los muchos subsistemas, es el que lanza la transacción comercial, transmite la información para realizar los demás procesos y sirve de interfaz entre las cajas registradoras, los sistemas de logística, los sistemas de contabilidad y otros sistemas empresariales.

Las funciones de los sistemas POS presentan distintos grados de sofisticación que van desde la realización de las operaciones más sencillas, a la gestión simultánea de una gran cantidad de tareas. Es posible que no todas las funciones que ofrece el proveedor se utilicen en el sistema que se entrega e instala en determinadas empresas. Los sistemas de capacidad mediana a alta presentan con frecuencia teclados o pantallas táctiles y permiten la conexión en red con ordenadores y sistemas de escaneo. La sofisticación y la variedad de este tipo de sistemas pueden suponer un desafío para el auditor fiscal que necesitará aprender a inspeccionarlos correctamente.

Auditoría de sistemas POS: el marco jurídico

Es esencial que en el marco jurídico para las auditorías se tengan en cuenta las necesidades de verificación que plantean los sistemas empresariales digitales, incluidos los puntos de venta. La mayoría de los países exige en sus legislaciones que las empresas

suministren la información comercial y los sistemas de contabilidad adecuados. Sin embargo, los empresarios tienen la libertad de establecer de manera independiente los sistemas que responden a estos principios. A continuación se presentan algunas de las características comunes de estas leyes y reglamentos:

- Los datos sobre la información comercial y los sistemas de contabilidad relacionados con las obligaciones tributarias deben conservarse durante un periodo determinado
- El propietario del negocio tiene la responsabilidad de garantizar que los registros contables estén organizados de tal modo que su auditoría requiera un tiempo razonable
- La conversión de datos electrónicos a formatos en papel está permitida, siempre que no dificulte la auditoría

En algunos países, entre ellos Noruega, existen reglamentaciones específicas para la contabilidad de empresas que manejan efectivo y utilizan sistemas POS. Este tipo de reglamentación puede especificar la manera de presentar los informes, el formato, el idioma y el periodo que debe conservarse la información.

Existe también otro grupo de países en donde la utilización de determinados sistemas POS certificados es obligatoria de manera generalizada o para cierto tipo de sectores minoristas o de prestación de servicios. Este método se conoce como la "caja fiscal" y más adelante, en la sección "Respuestas Gubernamentales", se describe con mayor detalle.

Requisitos de auditoría fiscal

Desde el punto de vista de la auditoría fiscal, los requisitos corresponden totalmente a las necesidades normales de una empresa en lo referente a la gestión de la información comercial. Además de las características antes mencionadas, entre los requisitos específicos para la auditoría fiscal se encuentran:

- la conservación electrónica de la información detallada de las transacciones;
- el suministro de registros detallados, si y cuando el auditor fiscal lo solicite;
- el mantenimiento de un seguimiento completo de las auditorías; y
- la instauración de medidas para impedir la alteración posterior de los datos con el fin de garantizar su integridad

La información detallada de los procesos comerciales es necesaria para realizar la auditoría de todas las ventas declaradas. Desde la perspectiva del auditor fiscal, las exigencias sobre la información comercial es relativamente sencilla; los registros de venta deben presentar de manera completa y correcta las transacciones de venta, y permitir a los funcionarios comprobar en un lapso de tiempo razonable que las cifras representan de manera completa y precisa las transacciones de venta. Así, los datos deben representar una imagen demostrable, completa y correcta de las ventas.

Las exigencias corresponden a los requisitos generales de todo negocio en relación con la tecnología utilizada para apoyar el sistema de negocios: desde el momento en el que se registra la transacción, se espera que la información quede correctamente almacenada. Asimismo se espera que las transacciones se vean reflejadas en los informes

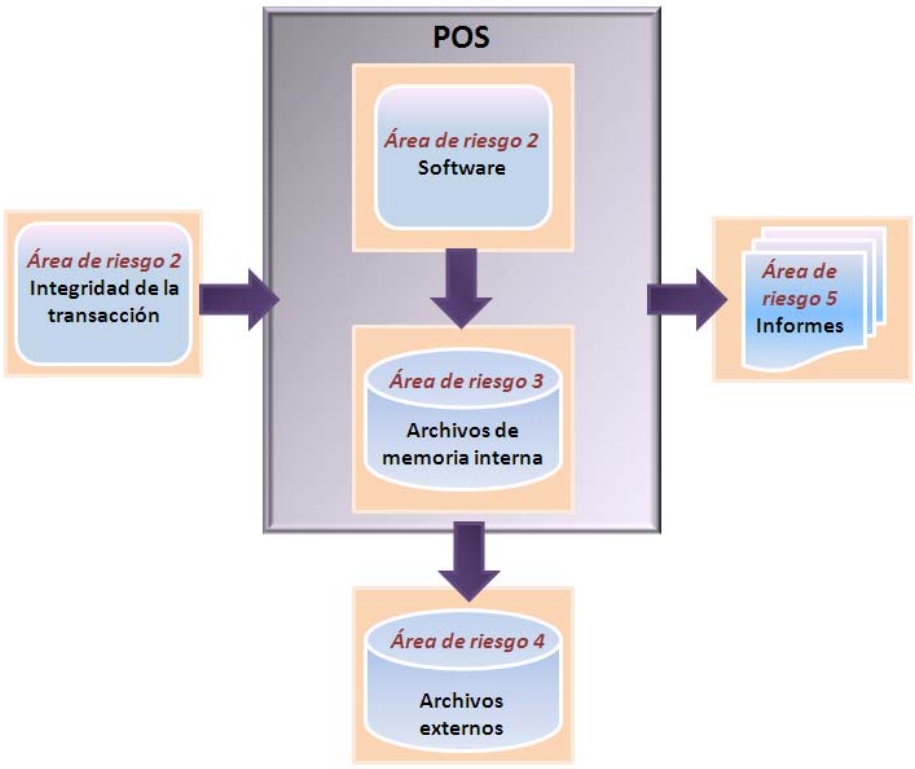
de manera completa y precisa. Los informes deberán poder elaborase en cualquier momento y al menos hasta el momento de la conciliación.

Las empresas más grandes toman las medidas adecuadas para proteger los datos almacenados, fundamentales para sus procesos. Los gerentes de estas empresas deben poder controlar los negocios, y para hacerlo, necesitan estos datos para sustentar las decisiones de rentabilidad a largo plazo y preparar los estados e informes financieros para los accionistas y las autoridades de reglamentación.

Riesgos de los sistemas POS

Las vulnerabilidades en materia de supresión electrónica de ventas pueden presentarse en áreas de riesgo específico de la configuración del sistema POS. Cada una de estas áreas de riesgo ofrece oportunidades para borrar o modificar los datos de las ventas, o incluso para eliminar por completo las transacciones. El siguiente diagrama[1] ilustra las cinco áreas de riesgo:

Figura 1. Modelo de riesgo del Sistema de Punto de Venta



Fuente: Información suministrada por Países Bajos

Integridad de la transacción. Para proteger la integridad de las transacciones, los parámetros de la caja registradora deben garantizar que la información sobre las transacciones sea completa, correcta y oportuna. Si no es así, el sistema produce información comercial poco fiable, lo que implica riesgos para la toma de decisiones adecuadas e impide la presentación precisa de declaraciones fiscales.

Software. El software debe estar diseñado para garantizar la integridad, la confidencialidad y la disponibilidad de los procesos realizados por el sistema de caja registradora. Si el sistema no puede garantizar la integridad, la confidencialidad y la disponibilidad, de nuevo, éste produciría información poco fiable para tomar las decisiones adecuadas y para la contabilidad fiscal. Es importante asegurarse de que el software funcione, sea capaz de almacenar toda la información sobre todas las operaciones efectuadas en el sistema de caja registradora y permita un seguimiento claro de las auditorías. Esto es necesario para poder gestionar y controlar todo el proceso comercial.

Memoria interna. Los datos de las transacciones, almacenados en la memoria y los archivos internos, son la base para todos los informes y corresponden a los datos que deberán verificarse en las auditorías e investigaciones. Ésta es el área de mayor riesgo de utilización de software de supresión electrónica de datos (u otros métodos de falsificación de archivos) para manipular la información almacenada en los datos de las transacciones.

Archivos externos. El riesgo se corre durante la transferencia y el almacenamiento de los datos de las transacciones en los archivos fuera de línea que se necesitan, por ejemplo, cuando el historial de la caja registradora electrónica (ECR) está lleno. En general, las leyes de los países exigen que las empresas mantengan por cierto tiempo los libros y cuentas correctamente, lo que implica también la existencia de soportes de datos para almacenarlos. De conformidad con algunas leyes, los libros y cuentas deben organizarse de tal modo que el auditor fiscal pueda revisarlos en un lapso de tiempo razonable. Los archivos externos también pueden ser archivos transferidos diariamente a partir del sistema POS que sirven de sistema auxiliar de gestión en un ordenador independiente, o de copia de seguridad para el sistema POS. Las copias de seguridad pueden almacenarse en un soporte externo o en un disco duro dentro del mismo sistema, pero en un archivo distinto. Éstas pueden contener información importante para descubrir la supresión electrónica de ventas en un sistema de caja registradora.

Informes. Esta área de riesgo está estrechamente relacionada con la segunda, el software que controla la elaboración de informes y por consiguiente permite la manipulación del diseño y la creación de éstos. Los informes son importantes para la gestión de una empresa y se utilizan para transmitir información al sistema de contabilidad, crear declaraciones fiscales y realizar otras operaciones. En caso de pérdida de los datos de las transacciones, es vital que el propietario de la empresa pueda recurrir a las copias impresas, las cuales contienen todas las transacciones introducidas y almacenadas en las cajas registradoras.

Notas

1. Los proveedores de sistemas POS en los Países Bajos en conjunto con las autoridades fiscales desarrollaron un modelo de los riesgos que suponen los sistemas POS con el fin de simular el cumplimiento de las obligaciones tributarias. Este trabajo forma parte del proyecto de los Países Bajos llamado "Quality Mark for Reliable POS systems" (Sello de Calidad para sistemas POS fiables) que se describe en el capítulo sobre Respuestas Gubernamentales. El grupo de expertos en supresión electrónica de ventas de la OCDE adoptó el modelo de los Países Bajos para crear un modelo general para el análisis de los riesgos de los sistemas POS.

Técnicas de supresión electrónica de ventas

El problema que plantean las técnicas de supresión electrónica de ventas es la enorme evasión fiscal que permite la no declaración de ventas y beneficios. En este capítulo se describe cómo las técnicas simples de captura (skimming), que aún se emplean, han sido automatizadas e integradas en los sistemas POS.

La supresión de ventas, también conocida como "captura" (skimmimg), se ha utilizado desde siempre de una u otra forma con el propósito, entre otras cosas, de evadir impuestos. La captura es un procedimiento simple que puede realizarse:

- omitiendo la introducción de las ventas en efectivo en la caja registradora, en cuyo caso el propietario del negocio conserva el dinero; o
- desviando las ventas a una segunda caja registradora no inscrita en los libros de contabilidad

Esta práctica es más frecuente en los negocios pequeños y medianos, puesto que en general los controles internos son escasos y los propietarios suelen controlarlos personalmente. En algunos casos, los negocios que recurren a la "captura" tienen dos juegos de libros y registros; uno para las autoridades fiscales y el otro para el propietario, quien en caso de venta del negocio querrá mostrar las cifras verdaderas al comprador potencial. En Australia, se descubrió un fraude en un restaurante que recurría a la captura de ventas mediante el cierre de las cajas registradoras a partir de cierta hora al final de la jornada. La enmienda de las cifras resultó en una deuda de 8,4 millones de dólares australianos para los propietarios del negocio, correspondientes a la evasión de impuestos y a las multas aplicadas.

Gracias a la tecnología, los negocios actuales han encontrado la manera de automatizar este tipo de fraudes valiéndose de programas informáticos de supresión electrónica de ventas, conocidos como "Phantomware" (software instalado directamente en el sistema POS) y "Zapper" (programas externos grabados en dispositivos USB). Este tipo de software ofrece la posibilidad de "capturar" las ventas en un entorno completamente informatizado, lo que permite al propietario llevar el negocio de manera totalmente normal en apariencia dado que los empleados registran todas las transacciones de venta en las cajas registradoras. La nueva tecnología permite al propietario efectuar supresiones electrónicas de ventas cuando mejor le convenga, normalmente al final de la jornada. La supresión puede corresponder a un importe preestablecido cada día o simplemente a un porcentaje de las ventas en efectivo. De este modo, ya no es necesario tener una "doble caja"; todo está completamente informatizado y disponible al propietario gracias a métodos relativamente sencillos para acceder al software de supresión, como por ejemplo una tarjeta magnética o un botón oculto en la pantalla para activar el menú especial. En algunos casos, los investigadores encontraron que la pulsación de un conjunto de teclas sirve también para activar el menú oculto.

Anteriormente, una cantidad importante de transacciones en efectivo era un indicio clave de todo tipo de "captura". Las transacciones de crédito y débito no solían prestarse para la "captura" ya que dejaban huella en el registro. Sin embargo, se han

encontrado indicios de que también se suprimen transacciones de débito y crédito. En varios países se están realizando investigaciones al respecto para comprobar si esta práctica anuncia una nueva tendencia. Si es así, se espera también identificar los elementos para combatirla, pero por el momento el trabajo está curso y no se tiene suficiente información para incluirla en el presente documento.

Según datos recopilados en Canadá y Estados Unidos, el costo de programas Phantomware o Zapper puede estar incluido en el costo del sistema POS, en particular cuando se trata de Phantomware, o puede elevarse a cerca de 1.500 dólares canadienses adicionales al costo del sistema POS.

Uso indebido de funciones del software de ECR y sistemas POS

Los sistemas POS modernos tienen numerosas opciones de programación y algunas de éstas pueden utilizarse para suprimir ventas. Un terminal POS puede programarse para:

- evitar que algunas operaciones tales como reembolsos, anulaciones y otras transacciones negativas, aparezcan en el informe o en el historial;
- evitar que algunas operaciones tales como reembolsos, anulaciones y otras transacciones negativas, se sumen a los totales finales;
- funcionar en modo de entrenamiento, ya sea para toda la caja o para algún empleado en particular, para que estas operaciones no aparezcan en los informes normales;
- reinicializar en cero o en algunos casos, en una cifra específica, los totales finales y otros contadores; y
- que ciertos artículos no aparezcan en el registro o en el historial

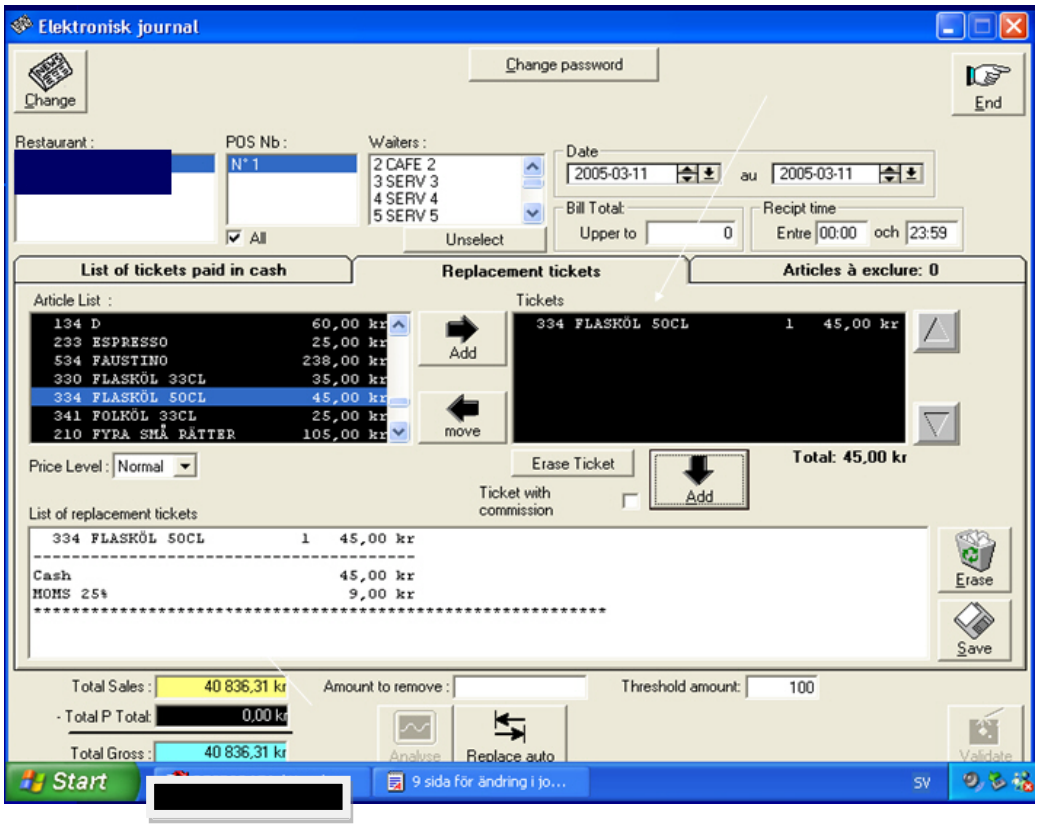
A diferencia de los programas Phantomware, las opciones del programa para seleccionar estas operaciones no están ocultas en la programación del menú y están descritas en el manual de utilización que el proveedor entrega; sin embargo, los clientes finales no suelen recibirlas y sólo se encuentran a disposición de los comerciantes oficiales. En la mayoría de las cajas registradoras, la programación se hace mediante la introducción de códigos que requieren cierto nivel de conocimientos en programación. La mayoría de los sistemas POS informáticos también incluyen opciones similares, pero los propietarios de negocios no necesariamente tienen los conocimientos técnicos para utilizarlas.

Phantomware

El Phantomware es un programa de software instalado o incorporado en la aplicación de contabilidad del programa de la ECR o del sistema POS informático. Se encuentra oculto para el usuario y puede accederse a él pulsando un botón invisible en la pantalla, introduciendo una secuencia de mando específica o introduciendo una combinación de teclas. Esta maniobra hace aparecer un menú de opciones para borrar selectivamente algunas transacciones de venta o para imprimir informes de venta omitiendo algunas líneas. Cuando se borran las ventas, la herramienta es capaz de ajustar automáticamente los detalles del inventario con el fin de evitar incoherencias aparentes. Así, en la opción para omitir líneas, únicamente el informe de ventas se ve alterado. Cuando hay cambios en la contabilidad, también es posible imprimir un listado de las

transacciones borradas para permitir al propietario del negocio la gestión (y el seguimiento) de los cambios. En Suecia, un hallazgo de este tipo sirve de ejemplo para ilustrar la práctica. En este caso se descubrió un programa para el sector de la restauración que recoge los datos del sistema POS informático y los guarda en un registro electrónico. La pantalla siguiente del sistema señala la posibilidad de cambiar rápidamente la operación, por ejemplo, la "lista de boletos pagados en efectivo" por "reemplazo de boletos".

Figura 2. Ejemplo de Phantomware



Fuente: Información suministrada por Suecia

En este ejemplo de Phantomware, las ventas no se borran, sino que se ajustan para sustituir artículos de mayor valor en el menú por artículos de menor valor. Este tipo de supresión electrónica de ventas es más sofisticado que el simple hecho de borrar la venta, y permite evitar los vacíos en la secuencia de transacciones que dejan las supresiones. Los auditores deben ser conscientes de que existe otro tipo de Phantomware capaz de borrar las ventas y renumerar las demás transacciones para crear secuencias consecutivas. Por lo tanto, la numeración consecutiva de las secuencias no excluye la utilización de métodos de supresión.

Programas Zapper

Los Zapper son programas de software externos que sirven para suprimir ventas. Estos programas se almacenan en algún tipo de soporte electrónico como dispositivos USB, CD y otros dispositivos extraíbles o pueden utilizarse en línea mediante enlaces en Internet. Tradicionalmente, los programas Zapper han sido diseñados, vendidos y actualizados por personas que desarrollan sistemas POS para determinados sectores, pero algunos contratistas independientes también han desarrollado este tipo de técnicas. La operación de estos programas es similar a la del Phantomware, pero es más difícil detectar su uso debido a su diseño sofisticado y porque no está instalado en los aparatos durante su operación normal. En Canadá se han descubierto casos de utilización de programas Zapper en varios restaurantes. En cada ocasión, el programa ha sido activado mediante un dispositivo USB que hace aparecer una pantalla especial en el sistema POS que permite al propietario del negocio borrar o modificar las transacciones de venta.

Resumen de las técnicas

Independientemente del tipo de programa empleado, los indicios sugieren que en la mayoría de los casos, el proveedor minorista del sistema POS lo ha programado para permitir la utilización fraudulenta. También es posible que brinden formación o suministren instrucciones escritas para su uso, lo que generalmente no implica ningún costo adicional para el cliente.

La interfaz de usuario de los programas Phantomware y Zapper es fácil de usar y por lo general tiene una apariencia profesional. Normalmente ha sido diseñada por alguien que trabajó en la creación del software operativo del sistema POS y su formato es similar al del sistema. Por este motivo, el software de supresión resulta familiar y parece tan legítimo como el software legal. Realizar las operaciones de cambio es generalmente sencillo; simplemente seleccionando el artículo que se desea borrar o reemplazar por un artículo de menor valor, o introduciendo el importe o el porcentaje de la venta que se desea "omitir". También es posible que haya filtros que permiten "omitir" cierto tipo de ventas. Así por ejemplo, si el propietario emplea a alguien ilegalmente, con el filtro puede borrar todas las transacciones efectuadas por ese empleado, o si vende productos de contrabando (por ejemplo, tabaco), puede "omitir" ese tipo de ventas para eliminar cualquier evidencia de participación en ese tráfico.

En resumen, las funciones de los sistemas de supresión electrónica de ventas son:

- acceso a software oculto;
- presentación de detalles de transacciones en efectivo (aunque actualmente también hay indicios de que las transacciones de crédito y débito son objeto de supresiones);
- eliminación de algunas transacciones de venta seleccionadas y de sus correspondientes registros;
- sustitución de ciertos artículos por artículos de menor valor;
- selección automática de artículos determinados para alcanzar un importe determinado (por ejemplo cuando el propietario desea encubrir retiros no declarados, por ejemplo, de 1.000 euros diarios, el software determina qué transacciones "omitir");

- eliminación del listado y otros rastros de transacciones; y
- almacenamiento de los datos originales en otro lugar

Por el momento no hay indicios de empresas que recurran a técnicas similares para inflar las ventas, por ejemplo, para lavar dinero de origen criminal. Sin embargo, es una posibilidad y las administraciones tributarias deben ser conscientes de este riesgo.

Estrategias de detección

Auditoría financiera

Las mejores prácticas en auditoría proporcionan métodos útiles para determinar si hay razones para sospechar que un negocio recurre a la supresión electrónica de ventas.

Box 1. Métodos de auditoría

- El cálculo del **consumo privado**, con base en los ingresos, los desembolsos en efectivo y las modificaciones en activos, sirve para establecer de cuánto dinero dispone el contribuyente para sus gastos personales. Si el cálculo del consumo privado resulta demasiado bajo o negativo, significa que el sospechoso ha gastado más dinero del que declaró disponer. Esto significa que puede haber ingresos no declarados correspondientes a entradas retenidas. Los métodos del patrimonio neto (Net Worth) y del depósito en efectivo (Cash Deposit) también son de gran ayuda.

- Cuando hay un **flujo negativo de fondos en efectivo** significa que el contribuyente sospechoso ha utilizado más efectivo de la caja registradora del que se supone que contiene. Esto es imposible y significa que existe una entrada de efectivo inexplicable u oculta.

- El análisis de los **beneficios brutos** sirve también para analizar las ventas. En primer lugar, se analizan las ventas calculando el beneficio bruto según la declaración oficial de las compras y los precios de venta del contribuyente. Luego se calcula el beneficio bruto a partir de las cifras registradas (compras y ventas) en los libros de contabilidad. Si el beneficio bruto registrado es inferior al beneficio bruto calculado teóricamente, quiere decir que no todas las ventas han sido registradas.

- El **control de volúmenes** se utiliza para analizar el flujo de mercancías. Este método ayuda a saber si el negocio está vendiendo más mercancías de las que ha comprado y tiene en reserva, lo que indicaría que hay ventas no registradas. Este método normalmente se utiliza con el análisis de los beneficios brutos.

- El cálculo de la relación **flujo de caja operativo / ventas netas**, corresponde al porcentaje del flujo de caja operativo neto con respecto a las ventas netas, a saber, los ingresos (de la declaración de renta). Cuanto mayor sea el porcentaje, mejor es el funcionamiento del negocio; una relación inferior de lo que se espera de un tipo de negocio en particular puede indicar una declaración incompleta de los ingresos. Cabe señalar que esta relación puede variar enormemente de un sector a otro y de una empresa a otra. En un caso del sector de la restauración, el porcentaje declarado no se desviaba de la norma nacional, pero en realidad, cuando se descubrieron las supresiones de efectivo, el porcentaje real era mucho más elevado, incluso por encima de la media superior de las estadísticas públicas.

- Las administraciones tributarias pueden recurrir también a **operaciones encubiertas** para observar el funcionamiento de un negocio. De este modo, los auditores pueden obtener valiosa información sobre la manera en que se está utilizando el sistema POS en la práctica. La administración tributaria puede hacerse pasar por un posible usuario y obtener copias del software en estudio para su análisis.

- Los **sistemas de gestión y de finanzas de una empresa**, tales como los sistemas de control de reservas y de facturación, suelen estar conectados al sistema de caja registradora. En una auditoría, la información que aportan puede ser importante para comprobar la fiabilidad de los datos de la caja registradora.

Los auditores pueden aprender a obtener información valiosa de los sistemas POS. Así, pueden aprender a reprogramar una ECR para revelar las ventas y transacciones suprimidas e imprimir los informes con los detalles. En el Reino Unido este enfoque ha sido adoptado y los auditores siguen una formación de tres días. La aplicación de este método en un proyecto local permitió inspeccionar el 68% de los casos en estudio.

Ciberauditoría

Los auditores del comercio electrónico o ciberauditores son conocidos también como Especialistas en Auditoría del Comercio Electrónico (Electronic Commerce Audit Specialists (ECAS) en inglés). Los sistemas POS suelen registrar miles de transacciones, lo que hace prácticamente imposible su inspección sin la utilización de técnicas y herramientas de auditoría asistida por ordenador (Computer Assisted Audit Tools and Techniques (CAATTs) en inglés) tales como IDEA. Este tipo de herramientas permiten a los auditores importar los datos de prácticamente cualquier formato o archivo, analizarlos y elaborar informes y gráficos (de los cuales se mostrarán algunos ejemplos más adelante). También sirven para realizar auditorías internas y análisis financieros normales y para identificar transacciones inusuales que podrían indicar actividades fraudulentas o de lavado de dinero. Los Especialistas en Auditoría del Comercio Electrónico (ECAS) son auditores con formación especializada en la utilización de técnicas y herramientas de auditoría asistida por ordenador (CAATT). Dado el uso de sistemas EPoS en muchas empresas que manejan efectivo, los ECAS tienen la responsabilidad de analizar y entender los complejos sistemas, así como de obtener la información clave que se comprobará con la ayuda de software de auditoría como IDEA, ACL o SESAM. La selección de los archivos de datos no es un procedimiento sencillo, en particular cuando un negocio utiliza ECR o un sistema híbrido, en lugar de un sistema POS informatizado. Además, los ECAS están suficientemente capacitados para analizar minuciosamente la gran cantidad de datos complejos de los sistemas EPoS y encontrar los indicios de supresiones electrónicas de ventas y otras infracciones. Asimismo, pueden compartir sus hallazgos con otros miembros del equipo de auditoría y compararlos con otras informaciones obtenidas por el auditor fiscal.

Peritajes informáticos

Los peritos informáticos se sirven de muchas de las herramientas que utilizan los ciberauditores. Con el fin de preservar la validez del peritaje es necesario proteger el sistema POS en cuestión en el laboratorio forense; es decir, así como en todo tipo de investigación criminal, es fundamental proteger las pruebas del caso, incluidas las herramientas utilizadas. Una vez que se han incautado los sistemas, normalmente de conformidad con una orden de allanamiento, éstos pueden duplicarse (clonación del disco duro original) y el peritaje puede comenzar.

Detección de rastros

La OCDE mantiene una lista detallada y confidencial de los rastros que los auditores, ciberauditores y peritos pueden identificar.

Técnicas de investigación penal

El papel del investigador penal en los casos de supresión electrónica de ventas, así como de cualquier otro tipo de evasión fiscal, consiste en dirigir la investigación de las finanzas de las empresas y los particulares sospechosos para procesarlos penalmente.

En el caso de la supresión electrónica de ventas, puede aplicar las técnicas tradicionales de investigación para recoger las pruebas valiéndose de instrumentos legales como órdenes de allanamiento (para incautar los sistemas POS, las copias de seguridad, los correos electrónicos y cualquier otro tipo de datos electrónicos), órdenes de divulgación u otras medidas administrativas para obtener información financiera; así como de entrevistas con posibles testigos, a saber, personas en el lugar de trabajo del negocio en investigación y otras personas como los fabricantes del sistema POS, entre otras.

El investigador penal también puede montar operaciones encubiertas o conjuntas con otros organismos de cumplimiento de la ley para vigilar a los fabricantes de sistemas POS. Aún cuando las operaciones encubiertas requieren mucha planificación y un elevado nivel de capacidades técnicas, el investigador puede obtener pruebas directas de un crimen y motivos razonables para solicitar órdenes de allanamiento. Además, la probabilidad de que los acusados acepten su culpabilidad también aumenta cuando se les presentan pruebas directas. En Canadá se llevó a cabo una operación encubierta para atrapar a un programador de software en la que los agentes se hicieron pasar por los ricos propietarios de un restaurante extranjero que buscaban implantar sucursales en Vancouver. En la operación, los agentes encubiertos negociaron la compra de un programa Zapper y las pruebas recogidas dieron motivos suficientes para emitir las órdenes de allanamiento de los locales del programador.

Cuando las pruebas demuestran la culpabilidad fuera de toda duda razonable, el caso se remite al fiscal para la imputación de delitos fiscales y otras acusaciones penales. El objetivo de todo procesamiento penal, además de castigar al infractor, es disuadir a otros de cometer infracciones similares y mejorar el cumplimiento de las normas haciendo saber que la evasión fiscal es un delito grave susceptible de procesamiento penal y público.

Investigación de rastros

Cabe suponer que cuando se utiliza un software de supresión electrónica de ventas para disimular el flujo de efectivo, determinar el ingreso real mediante una auditoría normal de los libros y registros es difícil, cuando no imposible. Según recientes investigaciones sobre Phantomware y sus conclusiones, resulta claro que los investigadores dependen en gran medida de los peritajes digitales para descubrir los hechos. Sin embargo, aún en ausencia de herramientas digitales, los auditores pueden valerse de sus habilidades informáticas para localizar y recuperar copias y archivos valiosos para la investigación.

Algunos casos registrados en Suecia y Noruega sirven de ejemplo para ilustrar cómo los cambios introducidos al software de supresión electrónica de ventas dificultan aún más la detección. Las primeras versiones de un programa Phantomware instalado en un sistema auxiliar de gestión dejaban una gran cantidad de rastros sobre las modificaciones hechas y el sistema conservaba los archivos con los datos de ventas originales. Las administraciones tributarias descubrieron la utilización de este software de supresión electrónica de ventas y el fabricante obtuvo la información sobre los hallazgos. En una investigación posterior se descubrió que el mismo programa había sufrido modificaciones para eliminar este tipo de rastros. Así, las versiones más recientes del programa eliminan la mayoría de los rastros de la venta original y tienen funciones para resistir una investigación digital tales como el cambio de fechados de los archivos y otro tipo de manipulaciones.

El poder jurídico y las capacidades técnicas para proteger el contenido de las cajas registradoras y los ordenadores tienen una importancia fundamental para detectar el uso de Phantomware y de programas de supresión electrónica de ventas. A pesar de que el software de supresión electrónica de ventas sea capaz de producir pruebas fehacientes para volúmenes de negocios reducidos y de eliminar todos los rastros del movimiento real, es probable que las pruebas electrónicas permanezcan ocultas en otros niveles tales como el sistema de archivos o el sistema operativo. En estos casos, la única opción es el peritaje digital.

La utilización de programas Zapper también puede dejar rastros en el sistema de archivos y en el sistema operativo, pero a diferencia del Phantomware, este tipo de programas desaparece del sistema luego de su utilización y es imposible analizarlo utilizando el material que normalmente se usa en los peritajes digitales. Si se encuentra un Zapper, éste se analiza, y en la mayoría de los casos la intervención del poder jurídico es necesaria para incautar los efectos personales.

Los peritajes digitales se realizan mediante la recopilación y el análisis controlados de los datos. Esto implica la incautación de las copias comprobables de las fuentes de datos que pueden estar relacionadas con el negocio y su análisis abarca los métodos de investigación y las medidas para interpretar la información digital incautada.

Incautación de las fuentes digitales

Si bien el objetivo principal de la incautación es el sistema POS, existen otras fuentes de información digital de un negocio relevantes para la investigación. Además del sistema POS, puede haber ordenadores con sistemas auxiliares de gestión y soportes externos de almacenamiento involucrados en el uso de Zappers y Phantomware. Partiendo de la base de que la incautación y revisión de dichas fuentes es legal, el desafío consiste en acceder a la información para copiarla. En ese caso se corre el riesgo de dañarla o borrarla, lo que puede tener graves consecuencias para la empresa investigada, y reducir la capacidad de investigar el volumen de negocios. Esto puede evitarse con cuidado y utilizando apropiadamente las herramientas y técnicas descritas más adelante.

Existe una amplia variedad de herramientas, equipos y software que pueden utilizarse para recopilar este tipo de datos. Estas herramientas garantizan básicamente que no se introduzcan modificaciones en la información digital del negocio y que la copia pueda compararse con la fuente original.

Cuando se necesita proteger el contenido de los sistemas propietarios, por ejemplo el de las cajas registradoras con ROM[1], deben llevarse a cabo pruebas preliminares en el mismo tipo de equipos antes de realizar la recopilación. Esto requiere buenos conocimientos sobre el tipo de tecnología del negocio antes de efectuar la investigación.

Las herramientas para proteger la información digital incluyen:

- El programa EnCase de Guidance Software, capaz de recopilar datos de diferentes soportes de almacenamiento, suele utilizarse con equipos que impiden nuevas inscripciones. El objetivo de impedir nuevas inscripciones es proteger la integridad de los datos originales.
- El programa Forensic Toolkit Imager de Access Data, que puede utilizarse con equipos que impiden nuevas inscripciones, recopila los datos de los sistemas en funcionamiento.

Estos son algunos de los ejemplos actuales y si bien los productos pueden variar, el principio es el mismo. Puede haber casos en los que las herramientas antes mencionadas no basten por sí solas y la capacidad de aplicar procedimientos de peritaje sea decisiva. En este contexto, la documentación debe ser de gran calidad y los procedimientos deben aplicarse siguiendo el principio de que las tareas deben poder verificarse y reproducirse posteriormente.

Análisis de la información digital

Los procedimientos para el análisis de la información protegida varían según las necesidades del caso, el acceso a los recursos y la experiencia y las normas que rigen este tipo de trabajo. Por consiguiente, resulta difícil hacer una representación general del análisis que debe realizarse, pero un buen punto de partida es la identificación de las entradas de lectura relacionadas con las ventas.

El peritaje debe empezar con la revisión y evaluación de toda la información sobre la auditoría fiscal en cuestión. Puede tratarse de información grabada en el sistema de almacenamiento, el sistema operativo, el software u otros archivos. El análisis debe centrarse en descubrir pruebas de la utilización de software de supresión electrónica de ventas y en determinar el software que se usó (Phantomware o Zapper).

Los archivos que contienen el registro de ventas deben compararse con los fechados[2] del sistema de almacenamiento y del sistema de archivos. La alteración de las ventas en un momento distinto al que debería inscribirse, puede indicar la utilización de software de supresión electrónica de ventas. Los archivos del historial también contienen datos susceptibles de revelar rastros que sustenten las supresiones indicadas. Normalmente, el sistema de archivos es una buena fuente de información para determinar el momento de creación, modificación y utilización de los documentos. Otra fuente de información puede ser el historial de entradas a las aplicaciones de protección tales como los programas antivirus, que proporcionan también datos sobre los nombres y el tamaño de los archivos. Las diferencias de tamaño de los archivos entre el historial del programa antivirus y el sistema incautado sirven para probar que el contenido ha sido cambiado. El análisis de este tipo de archivos busca principalmente identificar la utilización de software de supresión electrónica de ventas.

Las herramientas típicas para analizar la información digital son:

- El programa EnCase de Guidance Software ofrece un amplio soporte para diferentes sistemas de almacenamiento y se adapta al análisis general de los datos digitales recopilados (*www.guidancesoftware.com/*).
- El programa Forensic Toolkit de Access Data ofrece soporte para los sistemas de almacenamiento más comunes y simplifica el proceso de búsqueda mediante la indexación de los contenidos de los datos digitales recopilados (*www.accessdata.com/*).
- El programa IDA de Hex-Rays ofrece amplio soporte para desglosar los archivos de aplicaciones (*www.hex-rays.com/idapro/*).
- El programa Forensics WinHex de X-Ways Software Technology es un editor hexadecimal con diversas funciones de peritaje (*www.x-ways.com/*).

Si el propósito del análisis digital es detectar la presencia de un software de supresión electrónica de ventas, el análisis debe centrarse principalmente en los archivos de programa y en las entradas al sistema operativo. El procedimiento para este tipo de análisis puede variar y combinar distintas habilidades. Uno de los enfoques más utilizado y efectivo consiste en recuperar el software de aplicaciones del material protegido y examinarlo. Esto se hace lanzando el programa en otro equipo o en un *ordenador virtual*. En varias ocasiones, este método ha permitido el descubrimiento de funciones ocultas. También es una muy buena manera de probar la capacidad del programa para reducir el tráfico de ventas mediante la utilización de otras funciones, no necesariamente ocultas. Un enfoque algo más complejo es la aplicación de métodos de desglose de los archivos del programa. Este método sirve para transcribir el contenido de los archivos del programa en un código de programación que facilita al investigador la lectura de las instrucciones del programa para la máquina. No obstante, es un procedimiento largo y los resultados son inciertos. Otro enfoque que ha dado buenos resultados es el de recuperar las ventanas de diálogo y los gráficos de los archivos del programa. Estos elementos revelan funciones ocultas y proporcionan referencias sobre las funciones relacionadas con la reducción de los datos de venta.

Notas

1. La memoria de sólo lectura (ROM) es una memoria informática que puede almacenar de manera permanente las aplicaciones y los datos grabados.
2. El fechado es el momento preciso de ocurrencia de un *evento*, por ejemplo una transacción de venta registrada en un ordenador.

Respuestas gubernamentales

Desde hace algunos años, la supresión electrónica de ventas en los sistemas POS ha venido desarrollándose y los gobiernos y administraciones tributarias son cada vez más conscientes de este fenómeno. El trabajo del Grupo de Trabajo sobre Delitos Fiscales y otros Delitos ha contribuido a sensibilizar acerca de este problema en varios países y en varios de ellos, ha servido para estimular las actividades para resolverlo. En el marco del primer Foro sobre delitos tributarios celebrado en marzo de 2011 en Oslo, se hizo una presentación de este trabajo que sirvió para atraer la atención de un público más amplio de funcionarios de las administraciones fiscales y de otros organismos de observancia sobre los riesgos de evasión fiscal.

El Grupo de Trabajo sobre Delitos Fiscales y otros Delitos realizó además una encuesta sobre las acciones gubernamentales de varios países, lo que permitió el análisis de las distintas respuestas para afrontar los desafíos y riesgos que supone la supresión electrónica de ventas.

Las distintas acciones pueden clasificarse en las siguientes categorías:

- refuerzo del cumplimiento de la ley;
- concienciación;
- detección, auditoría e investigación;
- recopilación de información (inteligencia); e
- implantación de cajas fiscales y sistemas POS certificados.

El problema de la supresión electrónica de ventas es complejo y requiere una solución que integre algunas o todas estas categorías. Por esta razón es importante adoptar un enfoque estratégico para desarrollar un conjunto de respuestas apropiado.

Enfoque estratégico

Algunas administraciones tributarias consideran el trabajo en este ámbito como parte de una estrategia más amplia, ya sea para colmar la brecha fiscal o para abordar el problema de la economía subterránea.

Con el fin de brindar una respuesta estratégica al problema de la supresión electrónica de ventas, la administración tributaria debe identificar la naturaleza de los riesgos a los que se expone, para lo cual el contenido de este informe y la valiosa información de otras administraciones tributarias con mayor experiencia en la materia, son de gran ayuda.

Las situaciones de riesgo pueden identificarse mediante una serie de auditorías especiales destinadas a cierto tipo de negocios, tanto a los que presentan factores de riesgo como a los que no lo hacen. Este enfoque se ha aplicado en distintos países y en varias ocasiones se han descubierto casos de supresión electrónica de ventas en ambos tipos de negocio. Ampliar la realización de auditorías de sondeo puede contribuir a

identificar qué sectores minoristas y de servicios presentan mayores riesgos. En varios países se le ha dado preponderancia a los restaurantes, pero las cadenas de supermercado pequeñas, las farmacias minoristas, los salones de belleza y otros negocios de prestación de servicios también representan un riesgo elevado.

Resulta importante entender la naturaleza del negocio con sistemas POS y conocer al proveedor del sistema POS, tanto a nivel nacional como internacional, y su respectiva participación en el mercado.

A través de su legislación, varias administraciones tributarias han declarado su firme intención de luchar contra la supresión electrónica de ventas. Para este fin, los fiscales deben poder contar con el respaldo de leyes que penalicen el suministro, la posesión y la utilización de software de supresión electrónica de ventas para perseguir a los proveedores deshonestos más rápidamente, pues a menudo el proceso toma demasiado tiempo. Esto serviría además para enviar una señal fuerte a los fabricantes y proveedores con intenciones de cometer alguna infracción. Irlanda introdujo hace poco este tipo de leyes[1], y en Estados Unidos, algunos Estados como Florida, Maine y Nueva York, están siguiendo el ejemplo.

Refuerzo del cumplimiento de la ley

En el informe *Monitoring Taxpayer's Compliance*[2] del Foro sobre la Administración Tributaria, se afirma que "en un mundo ideal, todos los ciudadanos y empresas cumplirían con sus obligaciones tributarias oportunamente y declararían y cancelarían voluntariamente y a tiempo sus deudas, todas éstas calculadas a cabalidad y con precisión de conformidad con la ley". El cumplimiento de los contribuyentes de las obligaciones básicas también pueden considerarse desde la perspectiva del cumplimiento intencional (a saber, *cumplimiento voluntario*) o del cumplimiento por obligación y verificación de la administración tributaria (a saber, *cumplimiento forzado*). En el contexto de la administración tributaria, esta distinción tiene mucha importancia ya que el "cumplimiento forzado" tiene un costo, a menudo significativo.

Cumplimiento voluntario

En el manual tributario de la OCDE sobre teneduría de registros[3] se describen las ventajas del cumplimiento voluntario así:

"El cumplimiento forzado mediante la realización de comprobaciones, auditorías y procesamientos es una manera costosa de mantener el nivel de cumplimiento. Por esta razón, la mayoría de las administraciones tributarias intentan maximizar el cumplimiento voluntario del contribuyente, incitándolo a cooperar y cumplir activamente las normas tributarias. El cumplimiento voluntario reduce los costos administrativos del sistema tributario, pero sólo funciona cuando las empresas aceptan sus principios y los requisitos de las normas son comprensibles y relativamente fáciles de observar. El cumplimiento voluntario es más eficaz…cuando los requisitos tributarios corresponden a los sistemas de registro y contabilidad existentes en las empresas. Si se parte de la base de que estos sistemas son fiables, los costos del cumplimiento tanto para las empresas como para las administraciones tributarias puede ser mínimo".

Con el propósito de aumentar la "colaboración en el cumplimiento", el Foro sobre la Administración Tributaria elaboró la Nota de Orientación *Guidance and Specifications for Tax Compliance of Business and Accounting Software*, en la que hace recomendaciones a las administraciones tributarias y a los programadores de software. Estas recomendaciones se aplican a todo tipo de software empresarial y de contabilidad y

por lo tanto incluyen también los sistemas POS y las cajas registradoras. Según la Nota de Orientación, toda administración tributaria afronta condiciones distintas según diferentes factores como la orientación de las políticas, la legislación existente, el tipo de administración y la cultura, los cuales deberán adaptarse para proporcionar la respuesta adecuada.

Algunas administraciones tributarias optan por establecer relaciones de colaboración en el cumplimiento o relaciones privilegiadas con las principales empresas contribuyentes. Estas relaciones se basan en la confianza mutua, la transparencia y el entendimiento. Las administraciones tributarias aportan una conciencia comercial, imparcialidad, proporcionalidad, apertura y sensibilidad, y las empresas contribuyentes, aceptan la divulgación y transparencia de sus actividades. Para las empresas, una de las ventajas de este tipo de relaciones es la puntualidad de las cuestiones tributarias. Las administraciones tributarias deben tener en cuenta la estructura del control interno de las grandes empresas antes de establecer relaciones privilegiadas. El software de contabilidad de una empresa (incluido el software de las cajas registradoras electrónicas y de los sistemas electrónicos de punto de venta) forma parte de dicha estructura. Para las empresas pequeñas y medianas, las administraciones tributarias suelen considerar sectores específicos y sus asociaciones para discutir sobre el cumplimiento de las normas y brindar acompañamiento preventivo sobre cuestiones tributarias. En Canadá y los Países Bajos por ejemplo, las administraciones tributarias han abierto discusiones con el sector de la restauración a través de eventos locales de debate sobre el cumplimiento de las normas.

Otro actor importante es el grupo de los programadores y proveedores de software para sistemas de caja electrónicos. Varias administraciones tributarias están estudiando la posibilidad de establecer relaciones privilegiadas con programadores y proveedores de sistemas POS. La idea sería crear un entorno comercial en donde la gran mayoría de los sistemas de caja electrónicos no aplique técnicas de supresión electrónica de ventas. Las administraciones intentan cooperar con estos actores para incitarlos a erradicar el software de supresión electrónica de ventas. De esta manera es importante, no sólo influir sobre el comportamiento de los contribuyentes, sino sobre el de los programadores y proveedores de software. Este enfoque, más colectivo y proactivo, podría ser más eficaz que el de auditorías aisladas. En este contexto, es elemental establecer las normas para las cajas registradoras electrónicas y lograr que los programadores y proveedores de software se comprometan a observarlas.

La administración tributaria de Irlanda, que sirve de ejemplo para ilustrar este enfoque, lanzó una campaña para instar al uso correcto de los sistemas de caja registradora destinada a tres actores principales: los propietarios de negocios (usuarios finales), los proveedores de sistemas de caja registradora y de software para éstos; y sus correspondientes organismos de representación. Las partes interesadas recibieron una carta con un nuevo folleto sobre el tema publicado por las autoridades fiscales de Irlanda (Irish Revenue Commissioners). En dicho folleto se explicaba claramente la reglamentación en materia de IVA de 2008 aplicable a cada una de las partes interesadas, y en particular, la obligación de mantener registros al utilizar cajas registradoras . La información también está disponible en el sitio web de la administración tributaria, consultable en *www.revenue.ie/en/tax/vat/leaflets/cash-registers.html*.

Sello de calidad

La administración de los Países Bajos adoptó un enfoque innovador en materia de cumplimiento voluntario que condujo a la creación de un certificado de calidad para los sistemas POS comercializados en ese país. Si bien por el momento, el sistema del sello de calidad[4] es propio de los Países Bajos, es posible adaptarlo a otras jurisdicciones. Una vez que el proceso se haya completado, valdría la pena examinar si es posible ampliar su alcance a nivel internacional. Las normas específica para los sistemas POS deberían poder aplicarse internacionalmente, lo que aportaría beneficios aún mayores, a saber, la reducción sustancial de las posibilidades de supresión electrónica de ventas, una mayor certeza para las administraciones tributarias, los programadores y las usuarios de software sobre el cumplimiento de las normas de calidad de los sistemas POS y la disminución de los costos de cumplimiento para todos.

La administración tributaria y los fabricantes de los Países Bajos participan en el proyecto de manera voluntaria. El proyecto ya está funcionando y cuenta con el apoyo de varios fabricantes. La idea es que los sistemas de caja registradora cumplan con las normas para obtener el Sello de Calidad. Asimismo, la organización encargada del Sello de Calidad, que establece los criterios que debe respetar el sistema y vigila que los fabricantes respeten las normas (y atribuyan correctamente el Sello de Calidad), es completamente independiente.

Figura3. El Sello de Calidad introducido en los Países Bajos

Fuente: *www.keurmerkafrekensystemen.nl*

La administración tributaria de los Países Bajos, dentro de su sistema de gestión de riesgos para las auditorías, tendrá en cuenta que los sistemas con el sello de calidad presentan un menor riesgo de fraude.

Concienciación

La concienciación sobre las repercusiones de la supresión electrónica de ventas, si se hace de manera planificada y progresiva puede resultar provechosa. En ocasiones, los medios de comunicación y los periodistas de investigación contribuyen a la concienciación. Así ha sucedido en Canadá, los Países Bajos y Noruega.

Vale la pena que las administraciones tributarias consideren la posibilidad de establecer el diálogo con las principales partes interesadas tales como los fabricantes, los proveedores y los representantes de los sectores comerciales. A través del diálogo, pueden asegurarse de que las partes interesadas entienden:

- la manera en que se aplica la legislación al hardware y software que utilizan;
- el comportamiento que el gobierno espera de ellos en la materia;
- cómo cumplir los requisitos jurídicos; y
- las posibles consecuencias de no respetar las normas.

Cuando la concienciación está dirigida al usuario final, el diálogo puede abordar específicamente:

- los requisitos jurídicos y contables de teneduría de libros y registros;
- la utilización de sistemas de caja registradora y el cumplimiento de las normas correspondientes; y
- las ventajas de cumplir para las dos partes (situación gana-gana): los empresarios obtienen la información comercial más reciente y las autoridades tributarias recopilan conocimientos sobre los sistemas utilizados y se aseguran de que el contribuyente representa un riesgo "menor" (lo que permite destinar los recursos de auditoría a casos que representan "mayores" riesgos).

Las herramientas de comunicación empleadas en este enfoque pueden ser folletos concretos sobre la utilización de sistemas de caja registradora, páginas web publicadas en los sitios web de la administración tributaria o campañas de concienciación más específicas.

Cuando la concienciación está dirigida al proveedor, la comunicación puede tratar sobre:

- las disposiciones jurídicas y contables para el desarrollo, la instalación y la utilización de sistemas de caja registradora;
- los requisitos específicos que debe satisfacer un sistema de caja registradora; y
- las ventajas de cumplir para cada una de las partes (situación gana-gana): por ejemplo, los programadores y proveedores compiten en igualdad de condiciones y las autoridades tributarias tienen una garantía de que se satisfacen los requisitos (lo que representa menores riesgos y permite destinar los recursos de auditoría a casos que representan "mayores" riesgos).

La mejor forma de comunicar es organizar reuniones colectivas con los organismos de representación y reuniones particulares con los proveedores.

También se pueden adelantar campañas de concienciación pública de los contribuyentes divulgando en los medios de comunicación los resultados de las investigaciones y las detenciones con el fin de instar al cumplimiento de las normas. En Canadá, el cubrimiento mediático y la divulgación de las condenas han contribuido en gran medida al éxito de su programa de investigaciones penales. En algunas ocasiones, como en el caso de utilización de programas Zapper, el cubrimiento mediático puede solicitarse cuando se ejecutan las órdenes de allanamiento y las investigaciones penales están en curso. La publicidad de los procesamientos y condenas forma parte integral del sistema de autoevaluación y tiene un gran efecto disuasivo. En la Figura 4. se presenta un ejemplo de cubrimiento mediático. Esta historia fue recuperada y retransmitida en un telenoticiero vespertino.

Figura 4. Zappers – Cubrimiento mediático

Fuente: Diario *The Province*, "Redada para descubrir el uso de software fraudulento; Algo huele mal en estos restaurantes (…y no es el sushi)" Primera página del Diario *The Province*, 11 de diciembre de 2008.

Auditoría e investigación

Las administraciones tributarias no sólo investigan casos particulares, sino que estudian y analizan la información obtenida para predecir posibles casos de supresión electrónica de ventas. La elección de los casos para aplicar este enfoque depende de distintos factores. La información que proporciona el software de análisis de riesgos (como el programa IDEA antes descrito) y lo que se sabe sobre los negocios y los sectores que mueven grandes cantidades de dinero desempeñan un papel importante. Las distintas señales que la

administración tributaria identifica también pueden conducir al descubrimiento de técnicas y software de supresión electrónica de ventas y de sus proveedores.

Gracias a la auditoría e investigación de los proveedores de sistemas sospechosos de supresión electrónica de ventas, es posible obtener listas de clientes e identificar a los usuarios del software. Esta información se utiliza también para desarrollar proyectos de auditoría teniendo en cuenta tipos específicos de cajas registradoras electrónicas y sirve para enterarse de las modificaciones introducidas en los sistemas en curso de investigación.

Los casos más graves deben perseguirse penalmente y tener una amplia divulgación para aprovechar el efecto disuasivo. Varias administraciones tributarias han creado programas de declaración voluntaria para instar a los contribuyentes a manifestarse y corregir su declaración fiscal.

Uno de los elementos clave para todas las administraciones en su lucha contra la supresión electrónica de ventas es la confianza en la capacidad de los agentes de inspección (auditores fiscales, ciberauditores, peritos informáticos e investigadores) de aplicar la estrategia. Asimismo habrá que encontrar los recursos necesarios y desarrollar las habilidades para desempeñar las funciones que se mencionan a continuación.

Auditores fiscales

De acuerdo con el enfoque basado en el "principio" de la lucha contra la supresión de ventas, según el cual las administraciones tributarias confían en que los contribuyentes cumplen con sus obligaciones tributarias, mantienen libros y registros exactos y completos y presentan informes precisos, el auditor debe comprobar varios elementos durante la auditoría y visitar las instalaciones del contribuyente para observar personalmente los sistemas POS y tomar nota (por ejemplo, del nombre del fabricante y de cualquier sistemas POS "fuera de servicio"), entrevistar al contribuyente y al personal (por ejemplo, sobre la utilización y las diferentes funciones del sistema POS, las funciones y responsabilidades del contribuyente y el personal con respecto a los procesos y controles internos de la empresa), realizar pruebas indirectas sobre los ingresos (por ejemplo, establecer el estado de origen y aplicación de los fondos o realizar un análisis del patrimonio neto) y verificar las salidas registradas en el sistema POS directamente (por ejemplo comparando un antiguo informe de ventas con las ventas en el momento de la visita).

Así como en el caso de detección de posible evasión fiscal o de remisión al programa de investigaciones penales de las administraciones tributarias o a la instancia jurídica apropiada, el auditor también debe estar atento al posible uso de software de supresión de ventas y tomar las disposiciones necesarias para que el auditor del comercio electrónico, o ciberauditor, pueda examinar el sistema POS por sí mismo.

De acuerdo con el enfoque basado en las "normas" (en contraposición al basado en el principio), la función del auditor tiene mayor alcance. Así, el gobierno impone a los usuarios la utilización de hardware y software "certificados por el gobierno" y la obligación de conservar cierto tipo de registros. Además de comprobar los elementos mencionados anteriormente, los auditores pueden tener que ajustar y supervisar de cerca las cajas registradoras electrónicas y el sistema POS para descartar toda manipulación física y auditar los registros. En algunos países, los ciberauditores participan también en esta labor.

Los auditores remitirán al programa de investigaciones penales de las administraciones tributarias o a la instancia jurídica apropiada, todos los casos sospechosos de evasión fiscal, incluidos los que implican la utilización de software de supresión de ventas.

Ciberauditores y peritos informáticos

El ciberauditor es un apoyo importante para el auditor fiscal que inspecciona sistemas POS, pues es él quien tiene los conocimientos para acceder al sistema del contribuyente y recuperar las copias electrónicas del registro del sistema POS que el auditor fiscal necesita.

No obstante, desde los años 90, cuando se descubrió el primer software de supresión de ventas, su papel ha dejado de ser pasivo para participar activamente en las actividades de auditoría. En los países en donde se ha creado este cargo, el ciberauditor ha adquirido habilidades para realizar sofisticadas tareas de investigación informática (a saber, descifrar contraseñas, descubrir combinaciones de teclas de funciones ocultas o detectar códigos alterados). Asimismo entrevista a los propietarios y al personal de los negocios sobre la operación del sistema POS. Sus hallazgos normalmente se remiten al auditor fiscal que los incorporará al informe de auditoría.

En los casos de abuso grave, el informe puede formar parte de la investigación penal y el papel del perito informático cobra relevancia. Este especialista, al igual que el ciberauditor, ha adquirido experiencia para recuperar y examinar los datos electrónicos en el marco de una investigación penal. Accede al sistema POS y a los ordenadores del contribuyente y se vale de distintos métodos forenses (por ejemplo, el análisis de fechados, así como de cuentas y sumas de verificación, la clonación del sistema para realizar pruebas, el examen de correos electrónicos incriminatorios y la recuperación de archivos y correos electrónicos y otros datos borrados) para ayudar a los investigadores penales a establecer el *mens rea* o la voluntad criminal para la inculpación. En este caso sus hallazgos también se remiten al investigador penal que los incorporará al informe de investigación.

Independientemente del enfoque que las administraciones tributarias adopten, los ciberauditores y los peritos informáticos desempeñan un papel fundamental para garantizar el éxito de su lucha contra la supresión electrónica de ventas. Asimismo resulta primordial que los ciberauditores y los peritos informáticos sean capaces de cooperar, tanto entre ellos como con la administración tributaria, para combatir esta práctica.

Investigación penal

La amenaza de investigación y proceso penal es el arma disuasiva más poderosa que las administraciones tributarias pueden utilizar contra los contribuyentes incumplidos y contra quienes utilizan técnicas de supresión de ventas. Del mimo modo que los demás casos de vigilancia del cumplimiento de la ley, debe haber pruebas de la voluntad criminal y establecerse el importe de los ingresos no declarados.

El investigador aplicará las técnicas tradicionales de investigación (órdenes de allanamiento legales, órdenes de divulgación y entrevistas con los principales miembros del personal, tanto del negocio en cuestión como del fabricante del software de supresión de ventas, etc.) con el fin de recoger pruebas. Sin embargo, otras técnicas pueden resultar útiles como las operaciones encubiertas (descritas anteriormente) o las operaciones conjuntas con otros organismos de reglamentación y vigilancia de la ley para proteger

pruebas importantes y demostrar la utilización de software de supresión de ventas para ocultar ingresos. Un objetivo complementario es erradicar la supresión electrónica de ventas mediante la concienciación pública acerca del fenómeno y la injusta ventaja que toman estos negocios con respecto a los demás. La divulgación de esta práctica también transmite el mensaje a otros infractores de que la administración tributaria tiene conocimiento de este tipo de conductas y no las tolerará. Quienes incurran en este delito, se exponen a duras penas y multas e incluso a condenas de cárcel.

Actividades de inteligencia

Además de los agentes de inspección antes mencionados, existen agentes que trabajan "entre bastidores" y sirven de apoyo a las actividades visibles de la lucha contra la supresión de ventas. Hay distintos tipos de agentes de inteligencia: desde los que utilizan la información pública (de fuente abierta) y la información recopilada internamente por los auditores e investigadores (como por ejemplo listas de clientes de los proveedores) para elaborar informes de inteligencia que ayudarán a decidir la orientación de las actividades, hasta los que tienen la experiencia para formar a los cuatro tipos de agentes de inspección para realizar sus tareas.

Para poder detectar e investigar las actividades sospechosas, hay que entender perfectamente el funcionamiento de los sistemas POS. La información sobre los distintos sistemas puede:

- recopilarse abiertamente y recuperarse de fuentes abiertas; u
- obtenerse de manera clandestina (por ejemplo, adquiriendo manuales técnicos de manera anónima).

Las bases jurídicas para la recopilación de información dependen de la legislación nacional. Varios sistemas se han establecido con base en la tradición jurídica y el respeto de los derechos del público. La mayoría de los países miembros de la OCDE separa la legislación relativa al cumplimiento de la ley y la legislación tributaria; y el intercambio de información entre las dos instancias está sujeto a una estricta reglamentación. Generalmente, la recopilación y el intercambio de información tienen lugar cuando hay sospechas razonables de que se ha cometido o se está cometiendo un delito. En los casos de manipulación y fraude con sistemas digitales como los sistemas POS, es esencial que los organismos gubernamentales y de cumplimiento de la ley cuenten con el respaldo jurídico necesario para recoger y analizar la información. De este modo, las autoridades podrán identificar los sistemas y el tipo de abusos y preparar la respuesta más adecuada.

Las administraciones tributarias pueden compartir su información con otras administraciones gracias a las medidas de intercambio de información tributaria existentes. En particular, el intercambio espontáneo de información sobre fabricantes internacionales ha resultado muy útil. En este sentido, el Convenio sobre Asistencia Administrativa Mutua en Materia Fiscal para facilitar el intercambio de información entre distintos países también ha sido de gran utilidad en casos recientes. Si bien no todos los Estados miembros lo han firmado, las adhesiones están en constante aumento.

Recopilación de información (inteligencia)

Las actividades de inteligencia son la base para determinar el alcance de la investigación. La información recopilada mediante las actividades de inteligencia no sirve de prueba en un proceso, pero ayuda al investigador a obtener pruebas válidas. El

investigador utiliza esta información para orientar la búsqueda; le sirve para determinar qué buscar y en dónde buscar.

Las características de los sistemas de supresión electrónica de ventas se prestan para realizar labores de inteligencia. Los métodos eficaces en esos casos son:

- Operaciones encubiertas: varios departamentos de investigación fiscal penal recurren a este método para realizar investigaciones secretas, las cuales requieren una planificación jurídica, técnica y operativa muy detallada. Los resultados de estas técnicas pueden compartirse, pero en algunas jurisdicciones, ciertas disposiciones como el respeto de la privacidad, pueden impedir la presentación, la aceptación y la utilización de la información obtenida de esta forma en un proceso penal.
- Los métodos técnicos para *recoger* información incluyen el control de las comunicaciones y la intervención de líneas, el seguimiento de vehículos, la vigilancia de habitaciones y otro tipo de "técnicas pasivas" (pasivas en el sentido en que no hay un momento en el que se revela la actividad o se interviene activamente). Este tipo de técnicas se utiliza para *obtener* información e incluyen medidas como la instalación de registradores de utilización en ordenadores, el pirateo de ordenadores y otras acciones más agresivas.
- Asimismo se acude a la consulta de informantes y fuentes confidenciales.

Biblioteca de información

Varios países han estado desarrollando una biblioteca con información útil sobre la auditoría e investigación de sistemas POS. A nivel nacional, la biblioteca puede contener, además de la información pública sobre los sistemas de POS comercializados, sus fabricantes y proveedores, información técnica procedente de auditorías e investigaciones. La disyuntiva de permitir el acceso o no a las administraciones tributarias de otros países a este tipo de recursos se plantea, pues las normas sobre la protección de datos y el intercambio de información podrían representar un obstáculo. Una solución podría ser la creación de una plantilla, según los acuerdos existentes entre los distintos países, que sirva para solicitar el intercambio de información sobre la supresión de ventas en sistemas POS entre las distintas bibliotecas.

Cajas fiscales y sistemas POS certificados

Los gobiernos han adoptado distintos enfoques para luchar contra el uso indebido de sistemas POS y la evasión de impuestos. Desde la "caja fiscal" utilizada originalmente en Italia que guarda los datos de las ventas en un dispositivo de almacenamiento al final de la jornada, al "software de sistemas POS certificado" desarrollado en Portugal que genera datos de ventas codificados con firmas digitales para validar las transacciones reales; las soluciones se han multiplicado y perfeccionado. Uno de los principales avances técnicos es que, en lugar de proteger los datos al final de la jornada como lo hacían los antiguos sistemas, los sistemas POS ahora pueden hacerlo desde que se crean. En el Anexo se hace una descripción detallada de las características de las cajas fiscales y los sistemas POS certificados.

En este informe no se hacen recomendaciones sobre ninguna solución técnica en particular, sino que se proporciona información sobre las distintas soluciones adoptadas. Parece que la tendencia más extendida es la protección de los datos de la caja registradora

al momento de su creación e incluye la aplicación de nuevas técnicas como el cifrado de datos y la utilización firmas digitales.

Notas

1. La legislación introducida en 2011 añade los siguientes delitos al estatuto:

   "b) [quien] posee o utiliza deliberadamente y a sabiendas, con el propósito de evadir impuestos, un programa informático o un componente electrónico que modifica, corrige, borra, cancela, oculta o altera de otro modo cualquier registro almacenado o guardado en cualquier tipo de dispositivo electrónico sin conservar los datos originales y las subsiguientes modificaciones, correcciones, cancelaciones, ocultaciones o alteraciones,

   bb) proporciona o facilita deliberadamente y a sabiendas, con el propósito de evadir impuestos, un programa informático o un componente electrónico que modifica, corrige, borra, cancela, oculta o altera de otro modo cualquier registro almacenado o guardado en cualquier tipo de dispositivo electrónico sin conservar los datos originales y las subsiguientes modificaciones, correcciones, cancelaciones, ocultaciones o alteraciones.

   La pena para estos delitos en sentencia sumaria para una infracción cometida a partir del 14 de mazo de 2008, es una multa no superior a 5.000 euros (3.000 euros para las infracciones cometidas antes de dicha fecha) –la cual puede reducirse a no menos de un cuarto de la multa– o a discreción del tribunal, un periodo de cárcel no superior a 12 meses, o bien ambos, y en sentencia condenatoria, una multa no superior a 126.970 euros o a discreción del tribunal, a un periodo de cárcel no superior a 5 años, o ambos".

2. OCDE (2008) *www.oecd.org/dataoecd/51/13/40947920.pdf*.

3. Manual tributario sobre teneduría de registros: *www.oecd.org/dataoecd/29/25/31663144.pdf.*

4. El folleto sobre el enfoque del Sello de Calidad, también disponible en inglés, puede consultarse en el sitio *www.belastingdienst.nl/download/1419.html.*

Conclusiones

Desde que el Grupo de Trabajo de la OCDE sobre Delitos Fiscales y otros Delitos lanzó sus actividades de concienciación sobre la supresión electrónica de ventas entre las administraciones tributarias, su labor para identificar y combatir esta práctica ha aumentado significativamente. Sin embargo, la sofisticación de las técnicas implementadas por los proveedores de sistemas POS para ocultar este tipo de evasión fiscal también se ha perfeccionado. Este informe proporciona asesoramiento a las administraciones tributarias para desarrollar sus estrategias de lucha contra la supresión de ventas y facilita información específica para ayudar a los auditores e investigadores fiscales a detectar, investigar y desmantelar la evasión fiscal.

Corresponde a cada administración fiscal evaluar los riesgos y aplicar la estrategia más efectiva y apropiada para solucionar el problema. Las recomendaciones que deben formar parte de dicha estrategia se presentan más adelante.

El trabajo del grupo de expertos que se ha reunido para elaborar este informe ha obtenido importantes beneficios durante el proceso. El intercambio de experiencias ha contribuido a identificar nuevas áreas de estudio y en algunas ocasiones, ha conducido a crear alianzas internacionales para combatir el delito, hasta el punto de permitir la cooperación para realizar redadas en locales y emitir órdenes de arresto transfronterizas. Estas actividades empiezan a dar sus frutos para reequilibrar la situación, pues hasta ahora los proveedores de Phantomware y Zappers han podido aprovechar la falta de comunicación entre los países para operar internacionalmente.

Recomendaciones

Las administraciones tributarias deben desarrollar una estrategia para abordar la cuestión de la supresión electrónica de ventas dentro del enfoque general del cumplimiento de las obligaciones fiscales teniendo en cuenta los riegos provocados por los sistemas de supresión electrónica de ventas, promover el cumplimiento voluntario de las normas y mejorar los métodos de detección y la aplicación de contramedidas. En este contexto, lo ideal sería conocer el funcionamiento del sistema antes de lanzarse a identificar las áreas de riesgo y asignar los recursos.

Las administraciones deben desarrollar un programa de comunicación con el objetivo de concienciar a todas las partes interesadas acerca de la naturaleza criminal de la utilización de este tipo de técnicas y de las graves consecuencias de investigación y procesamiento judicial.

Las administraciones tributarias deben examinar si su poder jurídico se adapta a las necesidades de auditoría y peritaje de los sistemas de punto de venta.

Asimismo deben invertir para capacitarse y adquirir las herramientas para realizar las auditorías e investigaciones de los sistemas de punto de venta, lo que incluye determinar el papel de los especialistas en ciberaudoría y contratar expertos para el peritaje de sistemas digitales siempre que proceda. También deben implantarse mecanismos para garantizar que los distintos expertos cooperen efectivamente para combatir la supresión electrónica de ventas.

Por su parte, las administraciones deben considerar la posibilidad de recomendar la creación de leyes para penalizar el suministro, la posesión y la utilización de software de supresión electrónica de ventas.

Anexo: Cajas fiscales y sistemas POS certificados

Cajas fiscales

Hace más de 25 años, se introdujo por ley en varios países mediante la obligación de cajas fiscales y su uso es objeto de un creciente interés. Se trata básicamente de cajas registradoras que cumplen ciertos requisitos técnicos para garantizar el almacenamiento de datos y el seguimiento de las operaciones del sistema. Su implantación empezó en 1983 en Italia, cuando el gobierno estableció la obligación a determinados negocios de emitir recibos de caja registradora fiscal con el fin de reducir la economía subterránea y las transacciones opacas. Grecia y otros países siguieron el ejemplo y adoptaron el mismo sistema. Cada gobierno determinó los elementos que el sistema debía registrar, cómo debía almacenar los datos y cómo debía presentar la información (informes, archivos y recibos). Así, el sistema debía ser capaz de producir formatos específicos para proteger las datos para las auditorías fiscales.

Entre los requisitos específicos se encuentran:

- la preservación electrónica de los datos detallados de las transacciones en formatos específicos, codificados de manera determinada en soportes de almacenamiento definidos;
- el suministro de registros detallados únicamente cuando el auditor fiscal lo solicite;
- la preservación del rastro de auditoría completo y en algunos casos, el seguimiento de las operaciones;
- la dotación del sistema con algún tipo de aparato de supervisión; y
- la instauración de otras medidas técnicas para impedir la alteración posterior de los datos de tal modo que su integridad esté garantizada.

Las primeras versiones de las cajas fiscales protegían los datos de las ventas al final de la jornada, pero el enfoque actual consiste en proteger los datos al momento de su creación.

El método de trabajo se puede describir de la siguiente manera: al final de cada jornada, el tiene el gerente debe producir un Z-report (informe financiero diario). El total de las ventas registrado en el informe se guarda luego en una memoria protegida, en donde los contadores se actualizan con los totales de venta de ese día en particular. Luego, en algunos países, los contadores incluyeron también el registro de boletos, los totales de reembolso y otras transacciones.

Al principio, la memoria protegida (ROM) se sellaba y protegía en la máquina directamente mediante su fijación en la estructura con resinas epoxídicas o de otro tipo. Cuando las cajas registradoras se volvieron más sofisticadas e informatizadas, la obligación de colocar la memoria protegida en la estructura del terminal desapareció y

ésta podía instalarse en una impresora independiente del sistema (conocida como impresora fiscal).

En el recibo emitido, se declara específicamente si se trata de un recibo fiscal, que representa un registro de venta o si es un recibo de formación, un recibo *pro forma*, o una copia. Los recibos fiscales presentan también un sello al pie con el logotipo fiscal, el cual debe llenar los requisitos específicos de fuente y diagramación.

Figura 5. Ejemplos de izquierda a derecha: Italia, Bulgaria, Grecia y Hungría.

Fuente: Información suministrada por Italia, Bulgaria, Grecia y Hungría.

Según el país, la certificación (que demuestra que el sistema cumple con los requisitos jurídicos) depende de la administración tributaria o de organismos de certificación privados.

La solución de la "caja fiscal" ha sido implantada en varios países, entre los cuales se encuentran Argentina, Brasil, Bulgaria, Grecia, Hungría, Letonia, Lituania, Malta, Polonia, Rusia, Turquía y Venezuela. Este tipo de sistema se adapta a las condiciones de ciertos países, si bien en algunos países en desarrollo el sistema carga automáticamente los datos de las transacciones al sistema informático de la administración tributaria.

Sistemas POS certificados

Más recientemente, varios países intentan mejorar el cumplimiento de los contribuyentes mediante la obligación de utilizar sistemas de caja registradora "certificados" en los negocios que manejan efectivo o en sectores económicos específicos (como por ejemplo el sector de la restauración). Este enfoque se caracteriza por la utilización de equipos adicionales que sirven para agregar una firma digital en algunos o todos los elementos de un documento mediante tecnologías de cifrado. Este sistema de

supervisión comprende un dispositivo de vigilancia para almacenar los datos de los recibos y las firmas y para actualizar los totales finales en una memoria protegida.

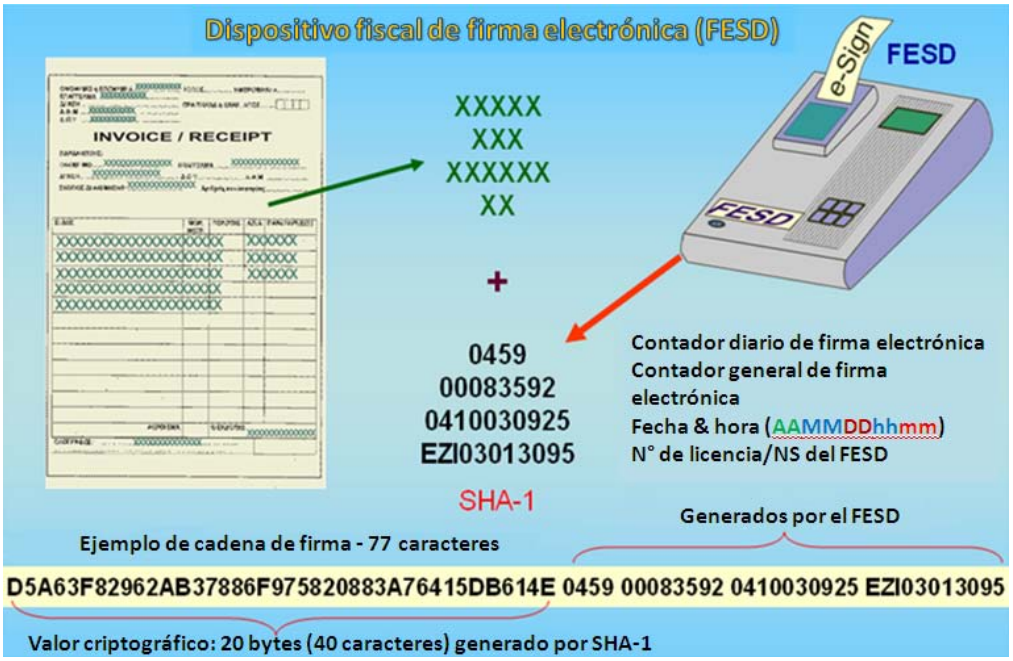
Firma de los datos de los recibos y almacenamiento de los datos importantes en un dispositivo de vigilancia

Las soluciones técnicas de este tipo no sólo sirven para agregar la firma digital en algunos de los recibos de venta, sino también para hacer un seguimiento adicional de los datos fiscales que contienen. Entre las administraciones tributarias que han implementado o están implementando este enfoque se encuentran Bélgica, Grecia, la Provincia de Québec en Canadá y Suecia.

Grecia

El Ministerio de Finanzas de Grecia fue el primero en introducir la firma digital[1] en los recibos y facturas. Cuando la firma se imprime en el recibo o factura y se almacena en el archivo de datos originales, se convierte en una herramienta eficaz para comprobar y garantizar la integridad de los datos del sistema POS.

Figura 6. Dispositivo fiscal de firma electrónica utilizado en Grecia



Fuente: Información suministrada por Grecia

Québec

El Gobierno de la Provincia de Québec diseñó un dispositivo de vigilancia llamado Sales Recording Module (Módulo de Registro de Ventas), que sirve para almacenar los datos importantes de los recibos y transacciones y generar una firma digital[2], la cual también aparece en el recibo del cliente en forma de código de barras bidimensional. En este caso, la administración tributaria, proveedor del Sales Recording Module, conserva la clave pública del dispositivo.

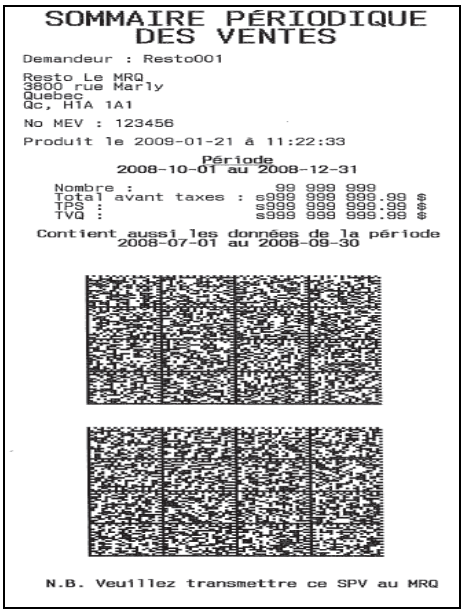
Figura 7. Módulo de Registro de Ventas utilizado en la Provincia de Québec

Fuente: Información suministrada por la administración tributaria de Québec

El escaneo del código de barras con un escáner de mano (con el software de clave pública) permite comprobar fácilmente si la firma es válida. Una firma inválida sólo puede significar que el contenido del recibo ha sido manipulado.

Adicionalmente, el Módulo de Registro de Ventas es capaz de generar un informe periódico con un código de barras bidimensional incorporado. Éste puede transmitirse a la administración tributaria de Québec por correo postal o por vía electrónica, haciendo una copia en un dispositivo USB y cargándola a través del servicio protegido de correo electrónico.

Figura 8. Ejemplo de un informe de los datos de venta con código de barras producido por el Módulo de Registro de Ventas de Québec


SOMMAIRE PÉRIODIQUE DES VENTES

Demandeur : Resto001

Resto Le MRQ
3800 rue Marly
Quebec
Qc, H1A 1A1

No MEV : 123456

Produit le 2009-01-21 à 11:22:33

Période
2008-10-01 au 2008-12-31

Nombre :	99 999 999
Total avant taxes :	$999 999 999.99 $
TPS :	$999 999 999.99 $
TVQ :	$999 999 999.99 $

Contient aussi les données de la période
2008-07-01 au 2008-09-30

N.B. Veuillez transmettre ce SPV au MRQ

Fuente: Información suministrada por Canadá

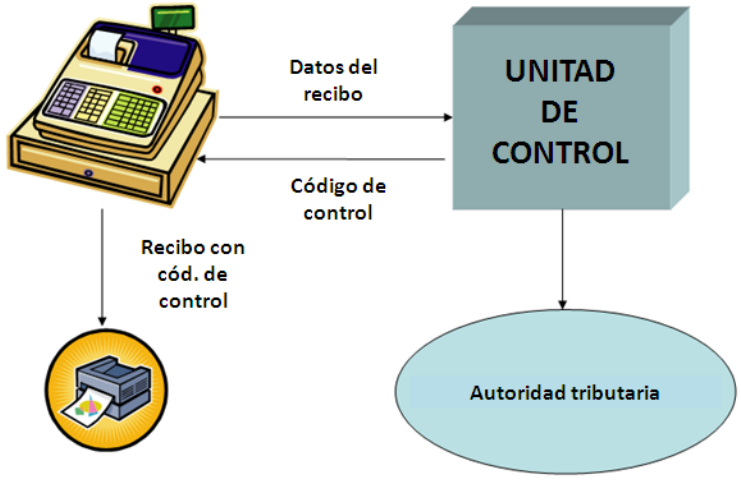
Este dispositivo ha sido implantado únicamente en el sector de la restauración. Para obtener mayor información, por favor visite el sitio web del Ministerio de Hacienda de Québec[3].

Suecia y Bélgica

La nueva legislación en Suecia, que entró completamente en vigor en 2010, introdujo la obligación de utilizar sistemas de caja registradora en los negocios que manejan efectivo (excepto en negocios pequeños, mercados al aire libre o grandes empresas con controles internos adecuados).

Según la legislación, los sistemas POS deben cumplir con estrictos requisitos técnicos, que incluyen tanto funciones obligatorias como funciones prohibidas. Además, el fabricante debe declarar la caja registradora a la administración tributaria.

Figura 9. Unidad de control implantada en Suecia



Fuente: Información suministrada por Suecia

Adicionalmente, debe instalarse una unidad de control conectada al sistema, la cual genera la firma digital[4] con base en el contenido del recibo. La firma (impresa en el recibo) permite comprobar fácilmente la integridad de los datos. Los datos importantes del recibo se conservan en una base de datos protegida en la unidad de control, la cual también contiene varios contadores que se actualizan con la emisión de cada nuevo recibo. Un sencillo procedimiento permite al auditor obtener una copia completa de la base de datos de la unidad de control, lo que facilita la auditoría mediante la utilización del software especialmente diseñado.

Bélgica está lista para introducir un sistema similar en 2013, pero por el momento, únicamente para el sector de la restauración. En principio, estará destinado a los restaurantes cuyo volumen de negocios anual corresponda al menos al 10% de sus ventas para consumo *in situ*.

La principal diferencia es que el dispositivo de vigilancia está compuesto de dos partes: un controlador de los datos de venta, similar a la unidad de control utilizada en Suecia; y una tarjeta de registro del IVA (VSC, por su sigla en inglés). El certificado con

la clave pública, proporcionado por la administración tributaria, estará incorporado en la tarjeta de registro del IVA, y quedará personalizado mediante la correspondencia del número de IVA con la tarjeta. De este modo, ambas claves quedarán registradas en la base de datos de la administración tributaria. Los fabricantes del controlador de los datos de venta no conocerán la clave.

Figura 10. El sistema de caja registradora certificado implantado en Bélgica

Fuente: Información suministrada por Bélgica

Este enfoque no sólo se centra en los aspectos técnicos, sino que implanta todo un procedimiento de certificación para cada elemento del "sistema de caja registradora certificado", lo que obliga a todos los actores (fabricantes, distribuidores, usuarios, administración tributaria) a tomar conciencia de sus responsabilidades en el proceso.

Al igual que en Suecia y Québec, la emisión del recibo (fiscal) es obligatoria y la administración tributaria publicará la lista de los sistemas certificados en su sitio web.

Actualmente, otros Estados Miembros de la UE están estudiando distintas modalidades de ambos conceptos, incluida la introducción de una función semi-en línea para controlar el módulo.

Firma de los datos de los recibos, almacenamiento de los datos importantes en un dispositivo de vigilancia y transmisión protegida en línea al gobierno

La firma de los datos de los recibos, su almacenamiento en un dispositivo de vigilancia y su puesta a disposición para las administraciones tributarias mediante el acceso a distancia (por ejemplo a través de GRPS), puede ser una solución económica y adecuada para algunos gobiernos. El acceso a distancia puede ser automático, es decir, en un momento dado se envía una copia completa a un servidor central de la administración tributaria; o por pedido, al momento de la auditoría. En ese caso, una descarga automática puede equivaler a una declaración fiscal oficial.

Firma del recibo con software de sistemas POS certificado

El sistema implantado en Portugal es el ejemplo más reciente para añadir una firma digital mediante software de sistemas POS certificado. Este enfoque, sin dispositivo de vigilancia, emplea un proceso de cifrado que firma los documentos mediante un par asimétrico de claves y un algoritmo RSA. El programador de software desarrolla una

clave privada que sólo él conoce y entrega una clave pública a la administración tributaria. La administración tributaria comprueba que el software cumple con todos los requisitos y en tal caso, lo certifica y divulga esta información.

Desde 2008, la utilización de sistemas POS conformes a la norma de auditoría para archivos de contabilidad (Standard Audit File for Tax purposes (SAF-T)) es obligatoria. Así, cada uno de los campos siguientes deberá tener firma: la fecha del recibo; la fecha de ingreso al sistema; el número del recibo; el total bruto; y la firma del documento anterior de la misma serie.

De este modo:

- es fácil ver en el recibo si se utilizó software certificado o no;
- los dígitos de la firma impresa deberán corresponder a la firma criptográfica de la SAF-T (cuando el auditor lo solicite); y
- con base en el examen de la clave pública, los datos y la firma del recibo, el analizador de la SAF-T podrá determinar:
  - si el recibo fue manipulado;
  - si la firma se generó con la clave privada correcta; y
  - si la secuencia de los recibos ha sido interrumpida.

Para mayor información y un análisis de firma gratuito, por favor visite el sitio web de la administración tributaria de Portugal: *http://info.portaldasfinancas.gov.pt/pt/apoio_contribuinte/news_saf-t_pt.htm*. También está disponible la traducción en inglés de la ley sobre certificación de software.

Notas

1. El algoritmo utilizado es un algoritmo SHA-1 de fuente abierta.
2. Este sistema utiliza una infraestructura de clave pública y un algoritmo RSA.
3. *www.revenuquebec.ca/en/a-propos/evasion_fiscale/restauration/secteur.aspx*
4. Un algoritmo RSA, una infraestructura de clave pública, una clave privada para el certificado de la unidad de control.

SUPRESIÓN ELECTRÓNICA DE VENTAS: UNA AMENAZA PARA LOS INGRESOS FISCALES

Las técnicas de “supresión electrónica de ventas” facilitan la evasión fiscal y tienen como consecuencia enormes pérdidas fiscales a nivel mundial. En el sector minorista, los sistemas de punto de venta son una herramienta importante que debe contener datos fiables. En realidad estos sistemas no sólo permiten “capturar” (skimming) los recibos de cobro tal como las cajas registradoras manuales, sino que una vez dotados de un software de supresión electrónica de ventas, facilitan fraudes mucho más elaborados. Las administraciones tributarias están perdiendo miles de millones de dólares y euros debido a las ventas no declaradas y a los ingresos ocultados mediante la utilización de estos métodos.

En este informe se describen las funciones de los sistemas de punto de venta y las áreas de riesgo específicas. También se exponen en detalle las técnicas de supresión electrónica de ventas que los expertos han identificado, en particular la utilización de programas “Phantomware” y “Zapper”, y se explica cómo los auditores e investigadores fiscales pueden detectar dichas actividades. En este informe, se examinan también unas estrategias adoptadas en diferentes países para combatir los abusos derivados de la supresión electrónica de ventas y se identifican algunas de las mejores prácticas. En particular, se hacen recomendaciones a los países que quieren abordar este ámbito importante de riesgo.

Índice:

www.oecd.org/ctp/taxcrimes