



CARTA A LOS MIEMBROS A.L.C. #43/10 (IML #40/10)

---

## El Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago Excluye de la Lista Aprobada Dos Equipos de Ingreso de PIN Comprometidos

---

**A: Miembros Principales  
Gerentes del Centro**

---

### En Breve

*Efectivo el 2 de abril del 2010, el Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago revocó la aprobación de los equipos de ingreso de PIN en el punto de venta Ingenico i3070MP01 y i3070EP01, que se han utilizado en ataques de adulteración y de skimming para capturar los datos de la banda magnética y el PIN. Estos equipos ya no están aprobados por Visa para nuevas instalaciones.*

---

El objetivo de esta comunicación es alertar a los adquirentes, procesadores y a sus comercios sobre equipos de teclado de PIN que recientemente fueron identificados como vulnerables y susceptibles a compromiso. Específicamente, los equipos de ingreso de PIN (PED) en el punto de venta (POS) de marca Ingenico, modelos i3070MP01 y i3070EP01 han sido usados en ataques de adulteraciones y skimming para capturar datos de la tarjeta con banda magnética y del PIN. Estos equipos han sido comprometidos en varios países; esta alerta aplica a todas las instalaciones.

Como precaución y para evitar futuras instalaciones, el Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago (PCI SSC), en coordinación con Ingenico, ha revocado la aprobación de estos dos equipos. **Efectivo inmediatamente, los modelos i3070MP01 y i3070EP01 de Ingenico ya no son terminales PED aprobados y han sido eliminados de la lista de aprobación de PCI SSC.**

### Impacto

Se aconseja a los adquirentes, procesadores y comercios identificar la ubicación de las versiones afectadas de estos PED e implementar controles adicionales en el punto de venta para evitar futuros ataques. Además, Visa recomienda enfáticamente que los adquirentes, procesadores y/o revendedores tomen las siguientes medidas:

- Informar a los compradores que estos equipos ya no están incluidos en la lista aprobada por PCI SSC
- Informar a los usuarios que estos equipos son objeto de ataques activos por parte del crimen organizado

- Informar a los usuarios sobre las medidas que se deben tomar para asegurar estos equipos

Los adquirentes, procesadores y comercios no deben comprar más terminales i3070MP01 y i3070EP01 de Ingenico. Los equipos que ya se hayan instalado o se encuentren en inventario y han sido revocados por el consejo PCI SSC pueden seguir instalándose.

### **Vulnerabilidad y Mitigación**

A nivel mundial aproximadamente 2.000 terminales i3070MP01 y i3070EP01 de Ingenico fueron adulterados, con lo que datos de la banda magnética y, en muchos casos, PINes quedaron comprometidos. Estos compromisos ocurrieron en Australia, Brasil y Canadá.

El método de ataque requiere que el delincuente se apodere del terminal durante varias horas, abra el equipo sin disparar los interruptores de seguridad, instale un dispositivo de skimming y devuelva el terminal al área de los cajeros sin detección. Una vez que el equipo ha sido adulterado, puede resultar difícil detectar visualmente el compromiso.

Se ha demostrado que el equipo de skimming captura los datos de la banda magnética así como los PINes ingresados por el cliente, permitiendo a los delincuentes crear tarjetas con banda magnética falsificadas. Aunque no hay evidencia de que los ataques han sido dirigidos a los datos de las tarjetas de chip, la evaluación técnica del equipo indica que también es posible obtener datos de las transacciones de tarjetas con chip. (Es posible que los datos de tarjetas de chip robadas sean utilizados para crear tarjetas de banda magnética; no obstante, cualquier tarjeta codificada con iCVV no sería susceptible a esta exposición.)

En las áreas donde se están desplegando tarjetas de chip, los adquirentes deben recordarles a los comercios que deben insertar las tarjetas de chip en terminales habilitados para leer chip (en vez de leer la banda magnética) para ayudar a evitar el skimming de la totalidad de los datos de la banda magnética. Los emisores deben emitir solamente tarjetas de chip utilizando iCVV y validar el CVV para cada transacción.

### **PCI SSC ha publicado mejores prácticas para la prevención de skimming que incluyen:**

- Inspeccionar regularmente los terminales para identificar cualquier anomalía, como sellos o tornillos que falten o hayan sido alterados, alambres raros, agujeros en el equipo, o adición de etiquetas u otro material que pudiera utilizarse para enmascarar el daño al equipo adulterado.
- Fijar físicamente los terminales y los teclados de PIN a los mostradores para evitar su remoción, así como asegurar las conexiones de cables.
- Asegurar físicamente bajo llave los terminales guardados que esperan ser instalados, y validar periódicamente el inventario a mano contra los registros de activos.
- Utilizar procedimientos de rastreo de activos en terminales para los equipos instalados, equipos que esperan ser instalados, equipos en reparación y equipos en tránsito hacia el lugar.

- Validar la identidad de los técnicos reparadores. Se debe negar el acceso al personal de servicio no autorizado o inesperado. Los técnicos de reparación autorizados y validados deben ser acompañados y supervisados.
- Pesarse periódicamente los equipos y comparar el resultado con el peso indicado en la especificación de los proveedores a fin de identificar equipos adulterados.

Los adquirentes deben incentivar a los comercios y agentes que ya han instalado los ahora revocados terminales i3070MP01 o i3070EP01 de Ingenico a considerar las siguientes mejores prácticas para ayudar a defenderse contra los ataques de skimming.

Muchos de estos puntos vulnerables también pueden resolverse si los terminales se instalan con un sistema de autenticación de terminal. En este caso, el sistema de computadora principal verifica continuamente que los terminales en línea estén funcionando correctamente. Si alguna vez se sustituye un terminal con un equipo no autorizado (o se desconecta, como sería necesario hacer para llevar a cabo este ataque), el sistema de computadora principal inmediatamente estaría al tanto de la adulteración.

Para los pedidos de terminales futuros, los adquirentes, procesadores y sus comercios solamente deben comprar aquellos equipos que estén actualmente incluidos en la *Lista de Equipos de Seguridad para Transacciones con PIN Aprobados por PCI SSC*. Como mejor práctica, Visa alienta a los adquirentes, procesadores y comercios a colaborar con los fabricantes de equipos y considerar la instalación solamente de las versiones más seguras (o las más recientes) de terminales para asegurar que los datos confidenciales de los tarjetahabientes sean debidamente protegidos.

#### **Información Relacionada**

Para mayor información, visite los siguientes sitios web:

- Sitio web de Visa sobre Equipos de Ingreso de PIN ([www.visa.com/PIN](http://www.visa.com/PIN)), haga clic en el enlace "Preguntas Frecuentes sobre PED en General"; o el sitio web de Visa sobre seguridad del PIN ([www.visa.com/cisp](http://www.visa.com/cisp)), haga clic en el enlace "Seguridad del PIN"
- [Sitio Web de Visa de Alineación de Seguridad del PIN de PCI](http://www.visa.com/pinsecurity) ([www.visa.com/pinsecurity](http://www.visa.com/pinsecurity)), haga clic en el enlace de la Versión 2.0 de "Requisitos de Seguridad del PIN"
- Suplemento de Información sobre PCI SSC: Prevención de Skimming—Mejores Prácticas para los Comercios ([https://www.pcisecuritystandards.org/pdfs/skimming\\_prevention\\_form.pdf](https://www.pcisecuritystandards.org/pdfs/skimming_prevention_form.pdf))
- El sitio web de PCI SSC sobre Seguridad de la Transacción con PIN ([www.pcisecuritystandards.org/pin](http://www.pcisecuritystandards.org/pin)), haga clic en el enlace "Lista de Equipos de Seguridad para Transacciones con PIN Aprobados por PCI SSC"

#### **Para más información**

Las preguntas relacionadas con la instalación de terminales específicos deben dirigirse a Ingenico.

Si tiene alguna pregunta sobre las políticas de Visa relacionadas con el uso de equipos aprobados, comuníquese con su Oficina Regional de Visa o envíe un correo electrónico a [pin@visa.com](mailto:pin@visa.com).

Cordialmente,

Jacinto Cofiño  
Jefe Regional del Departamento de Riesgos del Sistema de Pagos  
Región América Latina y el Caribe