



Manual de Instrucciones P2PE (PIM)

Guía para comerciantes sobre la implementación y el mantenimiento de la solución de reducción del ámbito de aplicación FreedomPay® P2PE

Versión 3.3

1. Información de la solución P2PE y datos de contacto del proveedor de la solución

1.1 Información de la solución P2PE

Nombre de la solución:	Plataforma de Comercio FreedomPay P2PE
Número de referencia de la solución según el sitio web de PCI SSC:	2022-00909.011

1.2 Información de contacto del proveedor de la solución

Nombre de la empresa:	FreedomPay, Inc.
Dirección de la empresa:	FMC Tower at Cira Centre South 2929 Walnut Street · Floor 14 Philadelphia, PA 19104
URL de la empresa:	http://corporate.freedompay.com
Nombre de contacto:	Matthew J. Donnelly
Número de teléfono de contacto:	+1-888-495-2446
Dirección de correo electrónico de contacto:	compliance@freedompay.com

P2PE y PCI DSS

Es posible que los comerciantes que utilizan esta solución P2PE deban validar el cumplimiento de PCI DSS y deben conocer sus requisitos aplicables de PCI DSS. Los comerciantes deben ponerse en contacto con su adquirente o con las marcas de pago para determinar sus requisitos de validación de PCI DSS.

2. Confirmar que los dispositivos no fueron manipulados y confirmar la identidad de cualquier personal de terceros

2.1 Instrucciones para garantizar que los dispositivos POI provengan únicamente de sitios/ubicaciones de confianza.

FreedomPay o su KIF certificado enviará por correo electrónico una notificación previa al envío al comerciante identificando los números de serie del dispositivo POI, el nombre del Mensajero de Confianza, el número de seguimiento, la Instalación del Proveedor Aprobado desde la que se envió el paquete y la Ubicación del Comerciante Aprobada a la que se envió el paquete.

Al recibir cualquier envío de dispositivos POI, el Comerciante debe:

- i. Inspeccionar el embalaje como se establece anteriormente.
- ii. Verificar que el mensajero identificado en el recibo de entrega sea un Mensajero de Confianza.
- iii. Verificar que el paquete fue enviado desde una Instalación de Proveedor Aprobada que se enumera a continuación:
 - a. FreedomPay Headquarters
2929 Walnut Street
Floor 14
Philadelphia, PA 19104
 - b. ScanSource
8650 Commerce Drive, Suite 100
Southaven, MS 38671
 - c. Ingenico Repair Facility
4020 Steve Reynolds Blvd
Norcross, GA 30093
 - d. Ingenico Headquarters
3025 Windward Plaza
Suite 600
Alpharetta, GA 30005
 - e. Brookfield Equinox / Expeditors International of Washington, Inc.
1621 W. Calle Plata Suite B
Nogales, AZ 85621
 - f. Equinox
9045 E. Pima Center Parkway
Suite 3
Scottsdale, AZ 85258
 - g. Ingenico Distribution Center
6430 Shiloh Road E, Suite B

Alpharetta, GA 30005

- h. Ingenico Warranty and Service Center
6190 Shiloh Crossing, Suite B
Alpharetta, GA, 30005
- i. POS Portal
1627 Main Ave.
Sacramento, CA 95838
- J. Pos Portal
1920 Watterson Trail Suite A
Louisville, KY 40299
- k. Maxwell Paper
435 College Street East
Belleville, ON K8N 5S7
Canada
- l. Ingenico UK
17 Ridge Way
Donibristle Industrial Park
Dalgety Bay, Fife KY119JU
United Kingdom
- m. First Data Hardware Services
1169 Canton Road
Marietta, GA 30066
- n. First Data Hardware Services
205 Export Blvd
Mississauga, ON L5S 1Y4
- o. ID Tech US KIF
10721 Walker Street
Cypress, CA 90630
- P. ID Tech TW_KIF
32F, 1080 Zhongsheng Road
Taoyuan District, Taoyuan City, Taiwan, R.O.C.
- q. Ingenico KIF Italia
Via Giorgio Stephenson 43/A
20157 Milano
Italia

r. CTDI Milton Keynes Ltd
Featherstone Rd,
Wolverton Mill,
Wolverton,
Milton Keynes
MK12 5TH,
United Kingdom

s. CTDI Soemmerda GmbH
Erfurter Höhe 10A
99610 Sömmerda
Germany

t. Zonal Retail Data Systems
Celestra, 1-5 James Way,
Bletchley, Milton Keynes MK1 1SU, United Kingdom
MK1 1SU

u. Zonal Retail Data Systems Ltd
4 Hutton Square
Brucefield Industrial Estate
Livingston EH54 9DJ

v. The Phoenix Group US
6705 Keaton Corporate Pkwy
O'Fallon, MO 63368

w. The Phoenix Group Canada
9-2785 Skymark Ave
Mississauga, ON L4W 4Y3

- iv. Verificar que los números de serie en el albarán de envío coincidan con los números de serie en la notificación por correo electrónico previa al envío.
- v. Actualizar el sistema de registro de dispositivos para reflejar el cambio en el estado y la ubicación del dispositivo.

El comerciante debe devolver inmediatamente a FreedomPay, como se establece a continuación, cualquier paquete de dispositivo POI que parezca haber sido manipulado, que haya sido entregado por alguien que no sea un Mensajero de Confianza o que haya sido enviado desde cualquier lugar que no sea una Instalación de Proveedor Aprobada.

Antes de devolver un dispositivo POI a una Instalación de Proveedor Aprobada, el comerciante debe enviar un correo electrónico a poidevicereturns@freedompay.com para determinar a dónde debe enviarse el dispositivo según la situación.

2.2 Instrucciones para confirmar que el dispositivo POI y el embalaje no fueron manipulados, y para establecer comunicaciones seguras y confirmadas con el proveedor de la solución.

Al recibir un dispositivo POI de FreedomPay, los comerciantes deben, como mínimo:

- Verificar que el mensajero identificado en el recibo de entrega sea un Mensajero de Confianza.
- Verificar que el paquete fue enviado desde una Instalación de Proveedor Aprobada.
- Verificar que los números de serie en el albarán de envío coincidan con los números de serie en la notificación por correo electrónico previa al envío.
- Verificar que el embalaje no esté dañado hasta el punto de exponer el interior del paquete.
- Verificar que el embalaje no se haya mojado hasta el punto de que la humedad haya penetrado las paredes del embalaje.
- Verificar que la integridad del embalaje a prueba de manipulaciones esté intacta.

Ejemplo de un paquete no manipulado con cinta a prueba de manipulaciones:



Si el dispositivo o el embalaje no pasan alguna de las inspecciones anteriores, póngase en contacto con su representante de FreedomPay y devuelva el dispositivo como se describe en la Sección 5.2.

Asegure físicamente los dispositivos POI en su posesión, incluidos los dispositivos:

- Esperando implementación
- En reparación o fuera de uso
- Esperando transporte entre sitios/ubicaciones

2.3 Instrucciones para confirmar la necesidad comercial y las identidades de cualquier personal de terceros que afirme ser personal de soporte o reparación, antes de otorgar a ese personal acceso a los dispositivos POI.

En la mayoría de los casos, FreedomPay podrá proporcionar soporte para dispositivos de forma remota sin requerir asistencia en el sitio. Sin embargo, durante instalaciones complejas o ciertos

casos de soporte, se puede enviar un técnico a la ubicación de un comerciante. En caso de que se necesite un técnico de FreedomPay en el sitio, asegúrese de que se sigan los siguientes pasos antes, durante y después de que se realice el trabajo en el sitio.

- i. Se asignará un técnico de campo a un caso y completará una solicitud de envío.
- ii. Una vez que se haya asignado un técnico, FreedomPay proporcionará al comerciante los detalles de la solicitud.
- iii. Cuando el técnico llegue al sitio, y antes de permitir el acceso al dispositivo POI, el comerciante debe verificar la identidad del técnico como empleado o contratista de FreedomPay. Se debe negar el acceso a todo el resto del personal sin una validación adecuada de su identidad.
- iv. Una vez que se haya verificado la identidad del técnico, el comerciante debe asignar un acompañante para monitorear la actividad del técnico en todo momento.
- v. Una vez que el técnico haya completado el trabajo, el comerciante debe responder al correo electrónico de envío con los siguientes detalles:
 - i. Forma de identificación presentada para verificación
 - ii. Tiempo empleado en la ubicación
 - iii. (Solo para casos de soporte) Número(s) de serie de la(s) terminal(es) tocada(s) por el técnico

FreedomPay nunca enviará técnicos al sitio sin coordinar previamente con los contactos del comerciante y proporcionar información sobre el técnico que se envía para fines de verificación. A cualquier persona que afirme ser un técnico de reparación/soporte sin la notificación o identificación adecuada no se le debe proporcionar acceso a los dispositivos POI.

3. Dispositivos POI aprobados, aplicaciones/software y el inventario del comerciante

3.1 Detalles del dispositivo POI

La siguiente información enumera los detalles de los dispositivos POI aprobados por PCI para su uso en esta solución P2PE.

Toda la información del dispositivo POI se puede verificar visitando:

https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php

Consulte también la Sección 9.2, "Instrucciones sobre cómo confirmar las versiones de hardware, firmware y aplicación en los dispositivos POI".

N.º de aprobación de PCI PTS:	Proveedor del dispositivo POI:	Nombre y número del modelo del dispositivo POI:	N.º de versión(es) de hardware:	N.º de versión(es) de firmware:
4-20324	Ingenico	<i>Lane/5000</i>	LAN51BA (cabezal MSR único), LAN51CA (cabezal MSR doble), LAN51DA (cabezal MSR único y cámara), LAN51EA (cabezal MSR doble y cámara)	820547v01.xx, 820376v01.xx, 820549v01.xx (SRED OnGuard FPE), 820556v01.xx (SRED OnGuard SDE), 820559v01.xx (SRED ANL), 820555v01.xx (SRED AWL)
4-30257	Ingenico	<i>Lane/8000</i>	LAN80AA	820547v01.xx
4-30326	Ingenico	<i>Link/2500</i>	LIN25AA (versión básica sin soporte CTLS), LIN25BA (versión básica con CTLS), LIN25CA (versión complementaria sin soporte CTLS), LIN25DA (versión complementaria con CTLS), LIN25EA (versión táctil sin soporte CTLS), LIN25FA (versión táctil con CTLS), LIN25GA (versión de cabezal doble sin soporte CTLS), LIN25HA (versión de cabezal doble con CTLS), LIN25IA (versión complementaria con conector trasero y sin soporte CTLS), LIN25JA (versión complementaria con conector trasero y con CTLS)	820547v01.xx
4-30237	Ingenico	<i>Lane/7000</i>	LAN70AA, LAN70AB	820547v01.xx

4-20316	Ingenico	<i>Move/5000</i>	(CTLS + Protector de privacidad) (CTLS) (Sin CTLS + Protector de privacidad) (Sin CTLS) MOV50AB, MOV50BB, MOV50CB, MOV50DB, MOV50JB (CTLS + Protector de privacidad + Tapa de la carcasa de escritorio)	820376v01.xx, 820547v01.xx, 820549v01.xx (SRED OnGuard FPE), 820555v01.xx (SRED), 820556v01.xx (SRED OnGuard SDE), 820559v01.xx (SRED ANL), 820565v01.xx (SRED FF1)
4-30310	Ingenico	<i>Lane/3000</i>	LAN30AA, LAN30BA, LAN30CA, LAN30DA, LAN30EA, LAN30FA, LAN30GA, LAN30HA	820547v01.xx, 820561v01.xx (firmware base)
4-20317	Ingenico	<i>DESK/5000</i>	(CTLS) (Sin CTLS + Protector de Privacidad) (Sin CTLS) DES50AB, DES50BB, DES50CB, DES50DB (CTLS + Protector de Privacidad)	820376v01.xx, 820547v01.xx (Firmware principal), 820549v01.xx (SRED OnGuard FPE), 820555v01.xx (SRED), 820556v01.xx (SRED OnGuard SDE), 820559v01.xx (SRED ANL), 820565v01.xx (SRED FF1)
4-30365	Ingenico	<i>Moby/5500</i>	MOB55xBxAx	BOOT: xxxx-F-801-01xx-xxxx-xx, CTRL: xxxx-F-802-01xx-xxxx-xx
4-30263	Ingenico	<i>Moby/8500</i>	MOB85AAx (w/o CTLS), MOB85ABx (w/o CTLS), MOB85ACx (w/o CTLS), MOB85BAx (w/ CTLS), MOB85BBx (w/ CTLS), MOB85BCx (w/ CTLS)	Boot: xxxx-F-701-01xx-xxxx-xx, Boot: xxxx-F-701-02xx-xxxx-xx, Boot: xxxx-F-701-03xx-xxxx-xx, Ctrl: xxxx-F-702-01xx-xxxx-xx, Ctrl: xxxx-F-702-02xx-xxxx-xx, Ctrl: xxxx-F-702-03xx-xxxx-xx, Ctrl: xxxx-F-702-04xx-xxxx-xx
4-30481	Ingenico	<i>Lane/3600</i>	LAN36AA2-xxxx, LAN36AB2-xxxx, LAN36BA1-xxxx, LAN36BA2-xxxx, LAN36CA1-xxxx, LAN36CA2-xxxx, LAN36CB2-xxxx, LAN36DA1-xxxx, LAN36DA2-xxxx, LAN36DB2-xxxx, LAN36EA2-xxxx, LAN36FA2-xxxx, LAN36AA1-xxxx	820571v01.xx (Firmware principal, 820376v12.xx (Servicios de seguridad), 820555v01.xx (SRED AWL), 820556v01.xx (SRED On-Guard SDE), 820549v01.xx (SRED On-Guard FPE), 820570v07.xx (Protocolos abiertos), 820565v01.xx (SRED FF1)
4-30381	Ingenico	<i>Self/2000</i>	SEL20AA	820566v01.xx
4-30393	Ingenico	<i>Self/4000</i>	SEL40BA	820547v01.xx

4-30384	Ingenico	<i>Self/5000</i>	SEL50CA	820566v01.xx
4-30510	Ingenico	<i>Self/3000</i>	SEL30BA1-xxxx SEL30BA2-xxxx SEL30AA1-xxxx SEL30AA2-xxxx	820571v01.xx (Firmware base), 820376v12.xx (Servicios de seguridad), 820555v01.xx (SRED AWL), 820556v01.xx (SRED On-Guard SDE), 820549v01.xx (SRED On-Guard FPE), 820565v01.xx (SRED FF1)
4-30535	Ingenico	<i>Self/4000 LE</i>	SEL41AA1-xxxx	820571v01.xx (Firmware principal), 820376v12.xx (Servicios de seguridad), 820556v01.xx (SRED On-Guard SDE), 820549v01.xx (SRED On-Guard FPE)
4-30532	Ingenico	<i>Self/5000 LE</i>	SEL51AA1-xxxx	820573v01.xx (Firmware principal), 820376v12.xx (Servicios de seguridad), 820556v01.xx (SRED On-Guard SDE), 820549v01.xx (SRED On-Guard FPE)
4-20359	Ingenico	<i>Move/5000</i>	MOV50BR (CTLS)	820547v11.xx, 820549v01.xx (SRED OnGuard FPE), 820556v01.xx (SRED OnGuard SDE), 820547v11.xx (Firmware principal), 820376v12.xx (Servicios de seguridad)

4-30494	Ingenico	<i>Lane/7000</i>	LAN70BD	820547v11.xx (Firmware principal), 820376v12.xx (Servicios de seguridad), 820555v01.xx (SRED AWL), 820556V01.xx (SRED On-Guard SDE), 820549V01.xx (SRED On-Guard FPE), 820565V01.xx (SRED FF1), 820548V07.xx (Protocolos abiertos), 820572V01.xx (Complemento Tetra JVM), 820376v14.xx (Servicios de seguridad)
4-30493	Ingenico	<i>Lane/8000</i>	LAN80BB	820547v11.xx (Firmware principal), 820376v12.xx (Servicios de seguridad), 820556V01.xx (SRED On-Guard SDE), 820549V01.xx (SRED On-Guard FPE), 820548V07.xx (Protocolos abiertos), 820376v14.xx (Servicios de seguridad)
4-30498	Ingenico	<i>AXIUM RX7000</i>	R70411xxxx	02.03.11.xxxxx (La solución SRED soportada por el firmware incluye SRED EP2, SRED C-TAP, SRED ZVT-H, SRED OnGuard FPE, SRED OnGuard SDE, SRED FF1)
4-30444	Ingenico	<i>AXIUM EX8000</i>	E801x2	01.09.11.xxxxx (with AP Solution 1, SRED EP2, SRED C-TAP, SRED ZVT-H, SRED OnGuard SDE, SRED OnGuard FPE, SRED FF1)

4-30443	Ingenico	<i>AXIUM DX8000-2, AXIUM DX8000-5</i>	D851x3 (con Solución AP 1)	01.09.11.xxxxx (con Solución AP 1 SRED EP2 SRED C-TAP SRED ZVT-H SRED OnGuard SDE SRED OnGuard FPE SRED FF1)
4-30527	Ingenico	<i>AXIUM RX5000</i>	R50411xxxx (sin protector de pin)	02.03.11.xxxxx (La solución SRED soportada por el firmware incluye: SRED EP2 SRED C-TAP SRED ZVT-H SRED OnGuard SDE SRED OnGuard FPE SRED FF1)
4-90075	ID Tech	<i>SREDKey 2</i>	80172001(Con MSR), 80172002(Sin MSR), 80172004(Con MSR), 80172005(Sin MSR)	SREDKEY2 FW v1.00.xxx.xxxx.S, SREDKey2 FW v1.01.xxx.xxxx.S
4-30432	Infinite Peripherals, Inc	<i>QuantumPay Reader 250</i>	06.00.xx.xx	3.0.xx.xx
4-30433	Infinite Peripherals, Inc	<i>QuantumPay Reader 300</i>	05.11.xx.xx	3.1.xx.xx, 3.2.xx.xx
4-30437	Infinite Peripherals, Inc	<i>QuantumPay PIN 400</i>	00xxxD1xxxxxx (non CTLS version) CLxxxD1xxxxxx (CTLS version)	3.1.xx.xx, 3.2.xx.xx
4-30438	Infinite Peripherals, Inc	<i>QuantumPay Connected 150</i>	PRR05xxx PRR15xxx PXR05xxx PXR15xxx	3.0.xx.xx, 3.1.xx.xx
4-30475	Infinite Peripherals, Inc	<i>QuantumPay Pro Plus</i>	21.1x.xx.xxx	SP: 3.0.xx.xx, AP: 1.0.xx.xx
4-80037	Castles Technology Co. Ltd	<i>Saturn 1000-E</i>	SATURN1000E-HW-V1.20.xxxx	1.1.1.xxxxxx
4-80033	Castles Technology Co. Ltd	<i>Saturn 1000</i>	SATURN1000-HW-V1.03.xxxx SATURN1000-HW-V1.01.xxxx SATURN1000-HW-V1.04.xxxx	1.1.2.xxxxxx 1.1.1.xxxxxx
4-30416	Castles Technology Co. Ltd	<i>Saturn 1000</i>	SATURN1000-HW-V2.00.xxxx	1.3.1.xxxxxx 1.4.1.xxxxxx
4-80075	Castles Technology Co. Ltd	<i>S1E2, S1E2-L, S1E2N</i>	HW-V1.00, S1E2: HW-V1.00	S1E2 & S1E2-L:

4-80094	Castles Technology Co. Ltd	<i>S1F4 PRO</i>	HW-V-1G.00	1.6.1.xxxxxx
4-80082	Castles Technology Co. Ltd	<i>S1P</i>	HW-V1.00	1.4.1.xxxxxx
4-80092	Castles Technology Co. Ltd	<i>S1P2</i>	HW-V-1D.00	1.6.1.xxxxxx
4-80091	Castles Technology Co. Ltd	<i>S1Mini2</i>	HW-V-1E.00	1.6.1.xxxxxx
4-30470	Elo Touch Solutions, Inc	<i>EMC0600, EMC0600C, EMC0600SC' EMC0600S</i>	A01.0EC.x A01.0NC.x A01.S00.x A01.SEC.x A01.SNC.x A01.000.x	5.xxx.xxx.xxx+ap 5.xxx.xxx.xxx+p 6.xxx.xxx.xxx+ap 6.xxx.xxx.xxx+p
4-90136	Ziosk	<i>Z600</i>	6.0.A 6.0.B	6201.29.xxxx.xxx.xxx 6201.30.xx.x.xxx
4-90335	Ziosk	<i>Z600 Pro</i>	6.0.A	6201.29.xxxx.xxx.xxx
4-30522	Verifone	<i>M425 M450</i>	H625-0007-0090-1xx-xxx-B0 (con protector de privacidad), H650-0007-0090-0xx-xxx-B0 (sin protector de privacidad), H650-0007-0090-1xx-xxx-B0 (con protector de privacidad), H625-0007-0090-0xx-xxx-B0 (sin protector de privacidad),	VOS3: 02.xx.xx, SPBL_01.02.xx.xx, SPFW_01.04.xx.xx, APFW_01.02.xx.xx, Android: 3.01D.xx
4-80062	Verifone	<i>P630</i>	H565-0007-xxxx-xxx-xxx-A1	Vault: APFW_01.02.xx.xx, VOS3: 01.xx.xx, Android: 3.01D.xx, Vault: SPFW_01.04.xx.xx

4-110000	Verifone	<i>V660P</i>	H660-0007-00D0-0Nx-xxx-B1, H660-0007-00D0-0Nx-xxx-B0	Vault: SPFW_01.06.xx.xx, Vault: APFW_01.03.xx.xx, Vault: SPFW_01.05.xx.xx, Vault: SPBL_01.02.xx.xx, Vault: SPFW_01.02.xx.xx, Vault: APFW_01.02.xx.xx, Android: 3.00D.xx, Vault: SPFW-01.04.xx.xx, Android: 3.01D.xx
4-30558	Verifone	<i>V660p-A</i>	H660-007-xxxx-xxx-xxx-A0	SPFW_01.05.xx.xx, SPBL_01.02.xx.xx, APFW_01.02.xx.xx, Android (VAOS):4.00F.xx, SPFW_01.06.xx.xx, APFW_01.03.xx.xx
4-80065	Verifone	<i>UX700</i>	U605-0007-xxxx-xxx-xxx-A0	Vault: SPBL_01.02.xx.xx, Vault: APFW_01.02.xx.xx, Vault: SPFW_01.06.xx.xx, Vault: APFW_01.03.xx.xx, Vault: SPFW_01.05.xx.xx, Android: 3.01D.xx, Vault: SPFW_01.04.xx.xx, VOS3: 02.xx.xx
4-40363	PAX Computer Technology (Shenzhen) Co Ltd	<i>A6650</i>	A6650-0xx-0x6-0xxx (NON-CTLS), A6650-0xx-0x6-1xxx (NON-CTLS), A6650-0xx-Rx6-0xxx (CTLS), A6650-0xx-Rx6-1xxx (CTLS),	26.00.01 xxxxx
4-30554	Toast Inc	<i>TG300, TG310</i>	REV1.xx	01.xx.xx.-10xxxxx

3.2 Detalles del software/aplicación POI

La siguiente información enumera los detalles de todo el software/aplicaciones (tanto aplicaciones P2PE como software P2PE sin pago) en los dispositivos POI utilizados en esta solución P2PE.

Todas las aplicaciones con acceso a datos de cuenta en texto claro deben ser revisadas de acuerdo con el Dominio 2 y están incluidas en el listado de la solución P2PE. Estas aplicaciones también pueden incluirse opcionalmente en la lista de Aplicaciones P2PE Validadas de PCI P2PE a discreción del proveedor o del proveedor de la solución.

Proveedor, nombre y n.º de versión de la aplicación	Proveedor del dispositivo POI	Nombre(s) y número del modelo del dispositivo POI:	N.º de versión de hardware y firmware del dispositivo POI	¿La aplicación está en la lista de PCI? (S/N)	¿La aplicación tiene acceso a datos de cuenta en texto claro? (S/N)
Ingenico, RA1v20.x Ingenico, UPP 1.1.x Ingenico, UPP 2.0.x	Ingenico	Lane 3000	N.º de hardware: LAN30AA, LAN30BA, LAN30CA, LAN30DA, LAN30EA, LAN30FA, LAN30GA, LAN30HA N.º de firmware: 820547v01.xx, 820561v01.xx (firmware base)	Sí. 2024-00470.056 Sí. 2023-00470.045 Sí. 2023-00470.051	Sí Sí Sí
Ingenico, RA1v20.x Ingenico, UPP 1.1.x Ingenico, UPP 2.0.x	Ingenico	Lane 5000	N.º de hardware: LAN50AB (sin CTLS), LAN50BB (CTLS) N.º de firmware: 820547v01.xx, 820376v01.xx, 820549V01.xx (SRED), 820555V01.xx (SRED), 820556V01.xx (SRED)	Sí. 2024-00470.056 Sí. 2023-00470.045 Sí. 2023-00470.051	Sí Sí Sí
Ingenico, UPP 1.1.x Ingenico, UPP 2.0.x	Ingenico	Lane 7000 v.5	N.º de hardware: LAN70AA, LAN70BD N.º de firmware: 820547v01.xx, 820555v01.xx (SRED AWL),	Sí. 2023-00470.045 Sí. 2023-00470.051	Sí Sí

3.2 Detalles del software/aplicación POI

			820556V01.xx (SRED On-Guard SDE), 820549V01.xx (SRED On-Guard FPE), 820565V01.xx (SRED FF1), 820548V07.xx (Protocolos abiertos), 820572V01.xx (Complemento Tetra JVM), 820376v14.xx (Servicios de seguridad)		
Ingenico, UPP 2.0.x	Ingenico	Lane 7000 v.6	N.º de hardware: LAN70BD N.º de firmware: 820376v12.xx (Servicios de seguridad), 820376v14.xx (Servicios de seguridad), 820547v11.xx (Firmware principal), 820549V01.xx (SRED On-Guard FPE), 820555v01.xx (SRED AWL), 820556V01.xx (SRED On-Guard SDE), 820565V01.xx (SRED FF1)	Sí. 2018-00470.020 Sí. 2023-00470.045 Sí. 2023-00470.051	Sí Sí Sí
Ingenico, UPP 1.1.x Ingenico, UPP 2.0.x	Ingenico	Lane 8000 v.5	N.º de hardware: LAN80AA N.º de firmware: 820547v01.xx,	Sí. 2023-00470.045 Sí. 2023-00470.051	Sí Sí
Ingenico, UPP 2.0.x	Ingenico	Lane 8000 v.6	820547v11.xx (Firmware principal), 820376v12.xx (Servicios de seguridad),	Sí. 2018-00470.020 Sí. 2023-00470.045	Sí Sí Sí

3.2 Detalles del software/aplicación POI

			820556V01.xx (SRED On-Guard SDE), 820549V01.xx (SRED On-Guard FPE), 820548V07.xx (Protocolos abiertos), 820376v14.xx (Servicios de seguridad)	Sí. 2023-00470.051	
RA1v20.x Ingenico, UPP 1.1.x Ingenico, UPP 2.0.x	Ingenico	Move 5000	N.º de hardware: MOV50AB, (Sin CTLS), MOV50BB, (CTLS), MOV50CB, (Sin CTLS + Protector de privacidad), MOV50DB, (CTLS + Protector de privacidad), MOV50JB (CTLS + Protector de privacidad + Tapa de la carcasa de escritorio), MOV50BR N.º de firmware: 820547v01.xx, 820376v01.xx, 820555v01.xx (SRED), 820549v01.xx (SRED OnGuard FPE), 820556v01.xx (SRED OnGuard SDE), 820559v01.xx (SRED ANL) N.º de hardware: MOV50AA (Sin CTLS); MOV50BA (CTLS), MOV50JA (CTLS), MOV50CA, MOV50DA, MOV50AB, MOV50BB (CTLS),	Sí. 2024-00470.056 Sí. 2023-00470.045 Sí. 2023-00470.051	Sí Sí Sí

3.2 Detalles del software/aplicación POI

			MOV50CB, MOV50DB (CTLS), MOV50JB (CTLS) N.º de firmware: 820548V06.xx, 820547v01.xx; 820376v01.xx; (SRED) CTLS: 820549V01.xx, 820555v01.xx (SRED), 820549v01.xx (SRED OnGuard FPE), 820556v01.xx (SRED OnGuard SDE), 820559v01.xx (SRED ANL), 820565v01.xx (SRED FF1), 820547v01.xx (Firmware principal), 820376v01.xx (Servicios de seguridad), 820376v02.xx (Servicios de seguridad), 820547v11.xx, 820549v01.xx (SRED OnGuard FPE), 820556v01.xx (SRED OnGuard SDE), 820547v11.xx (Firmware principal), 820376v12.xx (Servicios de seguridad)		
RA1v20.x Ingenico, UPP 1.1.x Ingenico, UPP 2.0.x	Ingenico	Link 2500	N.º de hardware: LIN25AA (versión básica sin soporte CTLS), LIN25BA (versión básica con CTLS), LIN25CA (versión complementaria sin soporte CTLS), LIN25DA (versión	Sí. 2024- 00470.056 Sí. 2023- 00470.045 Sí. 2023- 00470.051	Sí Sí Sí

3.2 Detalles del software/aplicación POI

			complementaria con CTLS), LIN25EA (versión táctil sin soporte CTLS), LIN25FA (versión táctil con CTLS), LIN25GA (versión de cabezal doble sin soporte CTLS), LIN25HA (versión de cabezal doble con CTLS), LIN25IA (versión complementaria con conector trasero y sin soporte CTLS), LIN25JA (versión complementaria con conector trasero y con CTLS) N.º de firmware: 820547v01.xx		
Ingenico, UPP 2.0.x	Ingenico	Self/2000, Self/4000, Self/5000, Self/4000LE, Self/5000LE	N.º de hardware: SEL20AA N.º de firmware: 820566v01.xx N.º de hardware: SEL40BA, SEL41AA1-xxxx N.º de firmware: 820547v01.xx, 820571v01.xx (Firmware principal), 820376v12.xx (Servicios de seguridad), 820556v01.xx (SRED On-Guard SDE), 820549v01.xx (SRED On-Guard FPE) N.º de hardware: SEL50CA, SEL51AA1-xxxx N.º de firmware: 820566v01.xx, 820573v01.xx	Sí. 2023-00470.051	Sí

3.2 Detalles del software/aplicación POI					
			(Firmware principal), 820376v12.xx (Servicios de seguridad), 820556v01.xx (SRED On-Guard SDE), 820549v01.xx (SRED On-Guard FPE)		
Ingenico, UPP 2.0.x	Ingenico	Lane/3600	Número de hardware: LAN36AA2-xxxx, LAN36AB2-xxxx, LAN36BA1-xxxx, LAN36BA2-xxxx, LAN36CA1-xxxx, LAN36CA2-xxxx, LAN36CB2-xxxx, LAN36DA1-xxxx, LAN36DA2-xxxx, LAN36DB2-xxxx, LAN36EA2-xxxx, LAN36FA2-xxxx, LAN36AA1-xxxx Número de firmware: 820571v01.xx (Firmware principal), 820376v12.xx (Servicios de seguridad), 820555v01.xx (SRED AWL), 820570V07.xx (Protocolos abiertos), 820565V01.xx (SRED FF1), 820556V01.xx (SRED On-Guard SDE), 820549V01.xx (SRED On-Guard FPE)	Sí. 2023-00470.051	Sí
Axium Retail Core Axium Payment Service (ARC APS)	Ingenico	AXIUM RX7000	Número de hardware: R70411xxxx Número de firmware: 02.03.11.xxxxx (La solución SRED soportada por el firmware incluye SRED	Sí. 2024-00470.059	Sí

3.2 Detalles del software/aplicación POI

			EP2, SRED C-TAP, SRED ZVT-H, SRED OnGuard FPE, SRED OnGuard SDE, SRED FF1)		
Axium Retail Core Axium Payment Service (ARC APS)	Ingenico	AXIUM EX8000	Número de hardware: E801x2 Número de firmware: 01.09.11.xxxxx (con solución AP 1, SRED EP2, SRED C-TAP, SRED ZVT-H, SRED OnGuard SDE, SRED OnGuard FPE, SRED FF1)	Sí. 2024-00470.059	Sí
Axium Retail Core Axium Payment Service (ARC APS)	Ingenico	AXIUM DX8000-2, AXIUM DX8000-5	Número de hardware: D851x3 (con solución AP 1) Número de firmware: 01.09.11.xxxxx (con solución AP 1, SRED EP2, SRED C-TAP, SRED ZVT-H, SRED OnGuard SDE, SRED OnGuard FPE, SRED FF1)	Sí. 2024-00470.059	Sí
Axium Retail Core Axium Payment Service (ARC APS)	Ingenico	AXIUM RX5000	Número de hardware: R50411xxxx (sin pinshield) Número de firmware: 02.03.11.xxxxx (La solución SRED soportada por el firmware incluye: SRED EP2, SRED C-TAP, SRED ZVT-H, SRED OnGuard SDE, SRED OnGuard FPE, SRED FF1)	Sí. 2024-00470.059	Sí
FreedomPay, FreeWay	Ingenico	Move 5000	Número de hardware: MOV50AB (Sin	Sí. 2025-00909.015	Sí

3.2 Detalles del software/aplicación POI					
Standalone Application (FSA) v3.0			CTLS), MOV50BB (CTLS), MOV50CB (Sin CTLS + Escudo de privacidad), MOV50DB (CTLS + Escudo de privacidad), MOV50JB (CTLS + Escudo de privacidad + Tapa de escritorio) Número de firmware: 820376v01.xx, 820547v01.xx, 820549v01.xx (SRED OnGuard FPE), 820555v01.xx (SRED), 820556v01.xx (SRED OnGuard SDE), 820559v01.xx (SRED ANL), 820565v01.xx (SRED FF1)		
FreedomPay, FreeWay Standalone Application (FSA) v3.0	Ingenico	Desk 5000	Número de hardware: (CTLS) (Sin CTLS + Escudo de privacidad) (Sin CTLS) DES50AB DES50BB DES50CB DES50DB (CTLS + Escudo de privacidad) Número de firmware: 820376v01.xx 820547v01.xx 820549v01.xx (SRED OnGuard FPE) 820555v01.xx (SRED)	Sí. 2025-00909.015	Sí

3.2 Detalles del software/aplicación POI

			820556v01.xx (SRED OnGuard SDE) 820559v01.xx (SRED ANL) 820565v01.xx (SRED FF1) 820548V02.xx (Protocolos abiertos), 820548V03.xx (Protocolos abiertos), 820548V05.xx (Protocolos abiertos)		
--	--	--	---	--	--

3.3 Inventario y Monitoreo de Dispositivos POI

- Todos los dispositivos POI deben ser documentados mediante procedimientos de control de inventario y monitoreo, incluyendo el estado del dispositivo (desplegado, en espera de despliegue, en reparación o fuera de uso, o en tránsito).
- Este inventario debe realizarse al menos una vez al año.
- Cualquier discrepancia en el inventario, incluyendo dispositivos POI faltantes o sustituidos, debe ser reportada a [FreedomPay, Inc.](#) a través de la información de contacto en la Sección 1.2 anterior.
- La tabla de inventario de muestra a continuación es solo para fines ilustrativos. El inventario real debe ser capturado y mantenido por el comerciante en un documento externo.

El comerciante debe implementar y mantener un sistema de seguimiento de dispositivos POI que identifique cada dispositivo POI según su estado actual. Ejemplos de posibles estados incluyen:

- Desplegado
- En espera de despliegue
- Fuera de servicio y/o en reparación
- En tránsito
- Retirado y devuelto

FreedomPay ofrece un sistema básico de registro a través de su Portal de Reportes Empresariales llamado Device Management Portal, que puede configurarse durante la implementación. Alternativamente, los comerciantes pueden implementar su propio sistema si lo prefieren. Los inventarios electrónicos de dispositivos POI deben almacenarse de manera segura, con acceso limitado únicamente al personal autorizado.

El comerciante también debe establecer un "sistema de contabilidad y control de estado" para realizar un seguimiento de todos los dispositivos POI (cantidad y tipo), registrar cambios en los inventarios materiales (entradas/salidas) y monitorear todos los aspectos del ciclo de vida del dispositivo POI mientras esté en posesión y control del comerciante. Registre todas las discrepancias

de inventario dentro de su sistema de control de inventario y reporte los dispositivos faltantes o perdidos a FreedomPay una vez identificados, enviando un correo a compliance@freedompay.com, o al socio/revendedor designado de FreedomPay que proporcionó los dispositivos.

Si su organización opera múltiples tiendas, a nivel regional o nacional, es importante emplear sistemas de gestión y seguimiento de inventarios a nivel local, regional y nacional para garantizar que se cumpla con el conocimiento y la capacidad de gestionar, rastrear y reportar inventarios en todos los niveles.

Se recomienda que el inventario de dispositivos contenga, como mínimo, información similar a la de la tabla de inventario de muestra a continuación. Toda la información de identificación específica del dispositivo requerida para el seguimiento del inventario se puede encontrar en una etiqueta en el panel trasero, en el compartimento de la batería de cada dispositivo POI (imágenes de la ubicación del número de serie para una muestra de dispositivos incluidas en el Apéndice C en la Sección 9, Guía Adicional) o a través de la interfaz lógica en el dispositivo POI.

El comerciante debe desarrollar y mantener protocolos escritos para la reubicación de dispositivos entre ubicaciones del comerciante. El comerciante debe monitorear y documentar el cumplimiento de dichos protocolos. Los protocolos de reubicación de dispositivos POI del comerciante deben ser al menos tan seguros como los protocolos identificados en este PIM para el envío de dispositivos POI hacia y desde las instalaciones de proveedores aprobados. Para obtener información adicional sobre cómo mantener la cadena de custodia para la reubicación o almacenamiento de dispositivos, comuníquese con compliance@freedompay.com o con el socio/revendedor de FreedomPay que proporcionó los dispositivos.

El comerciante puede ser solicitado para enviar su inventario anual de dispositivos POI a su adquirente como parte de su cumplimiento anual con PCI DSS. El incumplimiento de los controles enumerados en este PIM puede resultar en la "Exclusión del Comerciante"; es decir, la suspensión del Programa de Reducción de Alcance P2PE de la Plataforma de Comercio de FreedomPay.

Si un comerciante ya no desea utilizar los dispositivos POI proporcionados por FreedomPay como parte de un Programa de Reducción de Alcance PCI P2PE debido a la exclusión del comerciante, la terminación del contrato, el cierre del negocio u otra razón, el comerciante está obligado a destruir de manera segura todos los dispositivos POI proporcionados por FreedomPay. La destrucción segura debe realizarse utilizando el servicio de destrucción segura de FreedomPay enviando una solicitud a fperecycleservices@freedompay.com, incluyendo el número de dispositivos y los números de serie de cada dispositivo. Una vez recibida, el equipo de Servicios Profesionales de FreedomPay responderá con más detalles. Para obtener más información sobre los posibles servicios de destrucción, comuníquese con su representante de FreedomPay.

Tabla de Inventario de Muestra

Proveedor del Dispositivo	Nombre(s) y Número(s) del	Ubicación del Dispositivo	Estado del Dispositivo	Número de Serie u Otro	Fecha del Inventario
---------------------------	---------------------------	---------------------------	------------------------	------------------------	----------------------

	Modelo del Dispositivo			Identificador Único	

4. Instrucciones de Instalación de Dispositivos POI

No conecte dispositivos de captura de datos de tarjeta no aprobados.

La solución P2PE está aprobada para incluir dispositivos POI específicos aprobados por PCI. Solo estos dispositivos indicados anteriormente en la Tabla 3.1 están permitidos para la captura de datos de tarjeta.

Si un dispositivo POI aprobado por PCI del comerciante está conectado a un mecanismo de captura de datos que no está aprobado por PCI (por ejemplo, si un SCR aprobado por PCI se conectó a un teclado que no estaba aprobado por PCI):

El uso de dichos mecanismos para recopilar datos de tarjetas de pago PCI podría significar que ahora se aplican más requisitos de PCI DSS para el comerciante.

No cambie ni intente cambiar las configuraciones o ajustes del dispositivo.

Cambiar las configuraciones o ajustes del dispositivo puede invalidar la solución P2PE aprobada por PCI en su totalidad. Ejemplos incluyen, pero no se limitan a:

- Habilitar cualquier interfaz del dispositivo o mecanismos de captura de datos que fueron deshabilitados en el dispositivo POI de la solución P2PE.
- Alterar configuraciones de seguridad o controles de autenticación en el dispositivo POI.
- Abrir físicamente el dispositivo POI.
- Intentar instalar aplicaciones no autorizadas en el dispositivo POI.

4.1 Instrucciones de instalación y conexión

Se recomienda que la instalación de cada dispositivo POI se asegure utilizando uno de los siguientes métodos o una alternativa aprobada por su Evaluador de Seguridad Calificado (QSA):

- i. El dispositivo debe estar físicamente montado o asegurado para evitar su extracción, manipulación o sustitución no autorizada. Métodos aceptables incluyen:
 - a. Montar el dispositivo en un soporte de seguridad PIN aprobado.
 - b. Asegurar el dispositivo utilizando un candado con cable conectado a la ranura de seguridad del dispositivo POI y asegurado permanentemente al mostrador u otro hardware seguro y físicamente fijo en el extremo opuesto del cable. Una amplia variedad de candados con cable están disponibles en la mayoría de los minoristas de computadoras, en línea o a través de FreedomPay. Comuníquese con su representante de FreedomPay si necesita ayuda para encontrar un candado con cable adecuado.
- ii. El dispositivo debe ubicarse de manera que pueda ser observado/monitoreado fácilmente por personal autorizado y en un entorno que disuada intentos de compromiso.

Pasos adicionales de implementación

- i. Al iniciar el dispositivo, el comerciante debe realizar los siguientes pasos:
 - a. Verificar que el número de serie mostrado coincida con el número de serie en la parte inferior del dispositivo.
 - Para obtener ayuda para localizar los números de serie en los dispositivos POI, consulte el Apéndice C en la Sección 9, Guía Adicional.
 - b. Actualizar el sistema de registro de dispositivos para reflejar el cambio en el estado y la ubicación del dispositivo.
- ii. El dispositivo debe utilizar uno de los siguientes tipos de comunicación/conexión:
 - a. USB
 - b. Serial
 - c. Ethernet
 - d. WiFi
 - e. Bluetooth
 - f. Celular

Otro: Para tipos de comunicación POI no listados anteriormente, el comerciante debe comunicarse con compliance@freedompay.com para recibir la aprobación oficial de cumplimiento de FreedomPay para el uso de dicho dispositivo por parte del equipo de cumplimiento de FreedomPay. El comerciante debe recibir, por escrito, una certificación oficial de FreedomPay que indique que el tipo de comunicación/conexión POI, que no está listado en la lista anterior, es un método aceptado para la solución P2PE de la Plataforma de Comercio de FreedomPay.

Nota: Solo los dispositivos POI aprobados por PCI listados en el PIM están permitidos para su uso en la solución P2PE para la captura de datos de cuenta.

4.2 Guía para seleccionar ubicaciones apropiadas para dispositivos desplegados

FreedomPay, reforzado por el PCI DSS, recomienda que todos los dispositivos desplegados estén montados de manera segura y sean fácilmente visibles para el personal para prevenir su extracción o manipulación no autorizada. El dispositivo debe ubicarse de manera que pueda ser observado/monitoreado fácilmente por personal autorizado y en un entorno que disuada intentos de compromiso.

En caso de que una implementación esté designada para uso no supervisado, se deben establecer procedimientos para mitigar el riesgo asociado con la implementación. Esto puede incluir cámaras de seguridad, inspecciones más frecuentes, controles de prevención de manipulación u otros métodos aprobados por su QSA.

Los dispositivos que no estén en servicio deben almacenarse de acuerdo con la metodología descrita en la Sección 3.3.

4.3 Guía para asegurar físicamente los dispositivos desplegados y prevenir su extracción o sustitución no autorizada

Se alienta a los comerciantes a montar los dispositivos en servicio en un soporte de seguridad para PIN aprobado o a asegurar el dispositivo utilizando un candado con cable conectado a la ranura de seguridad del dispositivo POI y asegurado permanentemente en el extremo opuesto del cable. Una amplia variedad de candados con cable está disponible en la mayoría de los minoristas de computadoras o en línea. Por favor, contacte a su Representante de FreedomPay o QSA si necesita ayuda para encontrar un candado con cable adecuado. Para implementaciones que no sean propicias para dispositivos montados (es decir, dispositivos independientes o escenarios móviles), se deben implementar procedimientos para mitigar el riesgo de manipulación o compromiso del dispositivo. Esto puede incluir la asignación del dispositivo al personal de la ubicación, inspecciones más frecuentes u otros procedimientos aprobados por el QSA.

El comerciante debe establecer un área de “almacenamiento seguro” para los dispositivos POI que no estén en servicio. Este almacenamiento se utilizará cuando los dispositivos POI sean recibidos de FreedomPay antes de la instalación, transferidos desde otras Ubicaciones Aprobadas del Comerciante, o retirados del uso activo. El almacenamiento seguro se define por PCI como un espacio o ubicación designada que tiene acceso físico controlado, donde el personal debe estar autorizado para obtener acceso y se deben implementar mecanismos/políticas para documentar todo acceso físico al área de “almacenamiento seguro”, incluyendo:

- Identificación del personal autorizado para acceder a los dispositivos
- Restricción de acceso únicamente al personal autorizado
- Mantenimiento de un registro de todos los accesos, incluyendo nombre del personal, empresa, motivo del acceso, hora de entrada y salida

El comerciante debe implementar una política de acceso al “almacenamiento seguro” antes de implementar la solución P2PE Validada por PCI de FreedomPay. Esta política debe incluir una descripción de qué y dónde se encuentra el área de almacenamiento seguro, así como los procedimientos establecidos para cumplir con los requisitos establecidos en esta sección.

5. Tránsito de Dispositivos POI

5.1 Instrucciones para asegurar dispositivos POI destinados a, y durante, el tránsito

Para garantizar la entrega segura de los dispositivos, se recomienda utilizar un servicio de mensajería confiable que permita el rastreo de paquetes y la confirmación de entrega. FreedomPay utiliza y recomienda los siguientes servicios de mensajería, aunque se permiten otros métodos seguros:

- FedEx
- UPS

- USPS (en ciertos escenarios)
- R&L Carriers
- DHL
- Ceva Logistics
- New World Transportation
- Purolator
- DPD
- Startrack
- APC

Todos los dispositivos enviados por y hacia el comerciante (incluyendo envíos entre ubicaciones del comerciante) deben ser empaquetados con embalaje resistente a manipulaciones.

Ejemplos de embalaje a prueba de manipulaciones incluyen sobres o bolsas con etiquetas serializadas que muestren de manera irreversible evidencia de cualquier intento de abrir el paquete. El embalaje a prueba de manipulaciones puede adquirirse en proveedores de suministros de oficina y estará etiquetado específicamente como "A prueba de manipulaciones" o "Resistente a manipulaciones". Los paquetes también pueden asegurarse con cinta de seguridad a prueba de manipulaciones alrededor de todas las aberturas.

Asegure físicamente los dispositivos POI en su posesión, incluyendo dispositivos:

- En espera de despliegue
- En reparación o fuera de uso
- En espera de transporte entre sitios/ubicaciones

5.2 Instrucciones para garantizar que los dispositivos POI sean enviados únicamente a sitios/ubicaciones confiables

Todos los dispositivos enviados al comerciante por FreedomPay utilizarán un servicio de mensajería confiable de FreedomPay. Los servicios de mensajería confiables de FreedomPay están listados a continuación y también pueden ser utilizados por los comerciantes para envíos entre ubicaciones:

- FedEx
- UPS
- USPS (en ciertos escenarios)
- R&L Carriers
- DHL
- Ceva Logistics
- New World Transportation
- Purolator

- DPD
- Startrack
- APC

Estos servicios de mensajería serán utilizados para entregar dispositivos a las direcciones comerciales proporcionadas por el personal del comerciante durante la incorporación. En el caso de envíos entre ubicaciones del comerciante, los dispositivos solo deben ser entregados a direcciones comerciales confiables. Todos los dispositivos enviados por y hacia el comerciante (incluyendo envíos entre ubicaciones del comerciante) deben ser empaquetados con embalaje resistente a manipulaciones.

Ejemplos de embalaje a prueba de manipulaciones incluyen sobres o bolsas con etiquetas serializadas que muestren de manera irreversible evidencia de cualquier intento de abrir el paquete. El embalaje a prueba de manipulaciones puede adquirirse en proveedores de suministros de oficina y estará etiquetado específicamente como "A prueba de manipulaciones" o "Resistente a manipulaciones". Los paquetes también pueden asegurarse con cinta de seguridad a prueba de manipulaciones alrededor de todas las aberturas.

6. Guía para Manipulación y Modificación de Dispositivos POI

6.1 Instrucciones para inspeccionar físicamente los dispositivos POI y prevenir el skimming, incluyendo instrucciones y detalles de contacto para reportar cualquier actividad sospechosa

Se puede encontrar orientación adicional para inspeccionar dispositivos POI en el documento titulado *Skimming Prevention: Best Practices for Merchants*, disponible en www.pcisecuritystandards.org.

Los comerciantes deben inspeccionar, como mínimo, lo siguiente, en un marco de tiempo apropiado basado en su perfil de riesgo (típicamente trimestral):

- ¿El cable USB/ethernet ha sido dañado o alterado de alguna manera?
- ¿El número de serie en el dispositivo coincide con el número de serie proporcionado por FreedomPay? (Consulte el Apéndice C para la ubicación del número de serie).
- ¿Los dispositivos POI activos están asegurados adecuadamente según el PIM?
- ¿Los dispositivos POI inactivos están almacenados de manera segura según el PIM?
- ¿El dispositivo POI ha sido dañado de alguna manera?
- ¿Está presente la pantalla "Secured by FreedomPay"?
- ¿Están intactas las medidas adicionales de detección de manipulación añadidas por el comerciante y anotadas en el inventario, como sellos de seguridad, etiquetas o marcas ocultas?

Ejemplos de Áreas de Inspección:

Verifique el punto de conexión para detectar cables/conexiones adicionales o hardware.



Verifique que los tornillos exteriores no hayan sido removidos.



Inspeccione los puntos de interacción para detectar superposiciones o herramientas insertadas.



Verifique que la pantalla "Secured by FreedomPay" esté presente.



Si un comerciante despliega un dispositivo POI de FreedomPay en un área que no es monitoreada físicamente por un empleado aprobado del comerciante, deben existir procedimientos apropiados para reducir la posibilidad de manipulación del dispositivo y, en el peor de los casos, el tiempo entre el compromiso y la detección. Consulte a su Evaluador de Seguridad Calificado (QSA) independiente para obtener información adicional sobre la inspección y monitoreo de dispositivos POI.

Cualquier instancia de manipulación del dispositivo debe ser reportada a FreedomPay, y cualquier dispositivo que haya sido o se sospeche que ha sido manipulado debe ser retirado del entorno POS inmediatamente y devuelto a FreedomPay según las instrucciones descritas en la Sección 5.2.

6.2 Instrucciones para responder a evidencia de manipulación de dispositivos POI

El comerciante debe devolver inmediatamente a FreedomPay, como se establece a continuación, cualquier dispositivo POI o paquete que contenga un dispositivo POI que parezca haber sido manipulado, que haya sido entregado por alguien que no sea un servicio de mensajería confiable, o que haya sido enviado desde cualquier ubicación que no sea una Instalación de Proveedor Aprobada.

Envío de Dispositivos POI:

- i. Los dispositivos POI solo pueden ser transportados por un servicio de mensajería confiable a una Instalación de Proveedor Aprobada listada en la Sección 4.2.
- ii. Los números de serie de los dispositivos que se devuelvan, junto con la razón para devolverlos, deben ser comunicados a RMA@freedompay.com, quien generará una etiqueta de envío para la devolución.

- iii. Todos los números de serie de los dispositivos POI deben estar impresos en la declaración de embalaje o en la etiqueta de envío.

El comerciante debe actualizar su sistema de registro de dispositivos para reflejar el cambio en el estado y la ubicación del dispositivo.

7. Problemas de Cifrado de Dispositivos POI

7.1 Instrucciones para responder a fallas de cifrado en dispositivos POI

En caso de una falla de cifrado indicada por la presencia de un código de error 266 o un mensaje de "P2PE Encryption Error", se recomienda que el comerciante:

- i. Revise todos los registros del sistema de Punto de Venta (POS) y las funciones de agrupación para la autorización de crédito y cualquier indicio de datos de tarjeta en texto claro.
- ii. Revise todos los reportes de liquidación del POS para asegurarse de que no haya datos de tarjeta sin cifrar presentes.

En caso de que se encuentren datos de tarjeta en texto claro, o haya una falla en un control de seguridad del dispositivo, o se sospeche o confirme el uso no autorizado de funciones administrativas sensibles, el comerciante debe contactar inmediatamente al soporte técnico de FreedomPay y seguir las instrucciones de solución de problemas que se encuentran en la Sección 7 de este documento.

Hasta que la funcionalidad de cifrado adecuada en el dispositivo haya sido restaurada y el dispositivo haya sido reautorizado por FreedomPay, el dispositivo defectuoso no puede ser utilizado para procesar transacciones, a menos que el comerciante solicite formalmente una suspensión del cifrado P2PE como se describe en la Sección 6.2.

8. Solución de Problemas de Dispositivos POI

8.1 Instrucciones para solucionar problemas de un dispositivo POI

Si un dispositivo POI está dañado, destruido, parece estar funcionando mal o requiere servicio, el comerciante debe seguir el siguiente proceso al interactuar con el personal de FreedomPay:

- i. Contacte al soporte técnico de FreedomPay al **888-495-2446** o por correo electrónico a techsupport@freedompay.com.
- ii. Si el técnico de soporte de FreedomPay determina que se debe enviar un técnico de campo, el técnico completará una solicitud de despacho.
- iii. Una vez que se haya asignado un técnico, FreedomPay proporcionará al comerciante los detalles sobre la solicitud de despliegue.
- iv. Cuando el técnico llegue al sitio, y antes de permitir el acceso al dispositivo POI, el comerciante debe verificar la identidad del técnico como empleado o contratista de FreedomPay. Todo otro personal debe ser negado el acceso a menos que se valide adecuadamente su identidad.
- v. Una vez que se haya verificado la identidad del técnico, el comerciante debe asignar un acompañante para monitorear la actividad del técnico en todo momento.

vi. Una vez que el técnico haya completado el trabajo, el comerciante debe responder al correo electrónico de despacho con los siguientes detalles:

- i. Forma de identificación presentada para la verificación.
- ii. Tiempo que el técnico pasó en la ubicación.
- iii. Número(s) de serie del(los) terminal(es) tocado(s) por el técnico.

Si un comerciante ya no desea utilizar los dispositivos POI proporcionados por FreedomPay como parte de un Programa de Reducción de Alcance PCI P2PE debido a exclusión del comerciante, terminación del contrato, cierre del negocio u otra razón, el comerciante está obligado a destruir de manera segura todos los dispositivos POI proporcionados por FreedomPay.

La destrucción segura de los dispositivos es obligatoria y debe utilizar estándares aceptados por la industria. Se debe proporcionar prueba de destrucción mediante un certificado de destrucción, el cual debe ser enviado a FreedomPay siguiendo el proceso de destrucción segura. Para obtener más información sobre los servicios de destrucción de dispositivos POI de FreedomPay, comuníquese con su representante de FreedomPay para más detalles.

9. Guía Adicional

Avisos y Reconocimientos

Este Manual de Instrucciones P2PE se proporciona de conformidad con los requisitos del PCI DSS. La implementación de los controles establecidos en este PIM es un requisito para el SAQ-P2PE de PCI DSS y la Declaración de Cumplimiento. El uso de cualquier dispositivo POI no aprobado por FreedomPay y/o cualquier incumplimiento de los requisitos establecidos en este manual es bajo el único riesgo del comerciante y puede resultar en el incumplimiento del SAQ-P2PE de PCI DSS, la pérdida de la calificación para la reducción de alcance de PCI DSS y/o la seguridad comprometida de los datos.

Al utilizar la solución de Reducción de Alcance P2PE de FreedomPay, el comerciante acepta que no modificará ni intentará modificar ninguna configuración de los dispositivos POI proporcionados por FreedomPay, incluyendo, sin limitación:

- Intentar habilitar cualquier interfaz del dispositivo o mecanismos de captura de datos que hayan sido deshabilitados en un dispositivo proporcionado por FreedomPay.
- Intentar alterar configuraciones de seguridad o controles de autenticación.
- Abrir físicamente cualquier dispositivo.
- Intentar instalar aplicaciones en cualquier dispositivo.

Para mantener la reducción de alcance ofrecida por la solución de FreedomPay, el comerciante reconoce que todas las transacciones con tarjeta de crédito deben ingresarse/deslizarse a través de un dispositivo POI aprobado para permanecer dentro del Programa de Reducción de Alcance P2PE. Las transacciones ingresadas por cualquier otro medio no están sujetas al Programa Validado P2PE aprobado por PCI SSC de FreedomPay.

FreedomPay ha implementado un mecanismo en su pasarela de pagos (Freeway) para rechazar transacciones que se envíen, sin cifrar, desde un dispositivo no aprobado por FreedomPay con una respuesta de "P2PE Device Error", también conocida como error 266. Estas transacciones no cifradas no se almacenan en el entorno de FreedomPay, pero pueden almacenarse en los registros generados por el Punto de Venta del comerciante, lo que pone al comerciante en riesgo de perder la reducción de alcance de PCI.

Si un comerciante acepta pagos por cualquier otro método fuera de la solución PCI P2PE de FreedomPay o no puede resolver ocurrencias regulares de errores 266 dentro de los 30 días posteriores a su generación, debe optar por salir del Programa de Reducción de Alcance P2PE de PCI utilizando el formulario de Solicitud de Exclusión del Comerciante (Apéndice A).

Restricciones por País/Región

En caso de que un país o región imponga restricciones sobre qué marca y modelo de dispositivo se puede utilizar dentro de sus fronteras, la siguiente tabla se actualizará:

País/Región	Marca del Dispositivo	Modelo del Dispositivo
Australia	Ingenico	Lane 5000, Move 5000
Australia	IDTech	SREDKey v2

9.2 Instrucciones para confirmar versiones de hardware, firmware y aplicaciones en dispositivos POI

Las versiones de hardware se pueden encontrar en la parte trasera de todos los dispositivos, en la etiqueta del fabricante que contiene el número de serie. Ejemplos de la ubicación de esta etiqueta se pueden encontrar en el Apéndice C.

Dispositivos Ingenico:

Para encontrar la versión del firmware, siga los pasos a continuación:

1. Desconecte el dispositivo del sistema POS u otro sistema frontal.
2. Encienda el dispositivo utilizando el cable de alimentación o conectándolo a una PC mediante el cable USB.
3. Durante el inicio del dispositivo, presione la siguiente secuencia de teclas en el dispositivo Ingenico: 2634, [Botón verde], F.
4. Si su dispositivo no tiene una tecla "F", la secuencia sería: 2634, [Botón verde], +.
5. Seleccione el siguiente menú: Panel de Control/Información del Terminal/Firmware PCI PTS/Mostrar.

6. Registre la información del firmware asociada con M1.

La versión de la aplicación cargada en los dispositivos Ingenico se puede ver en la pantalla de inicio durante el arranque del dispositivo. El valor de "Versión PCI" debe coincidir con la plantilla de número de versión mostrada en el sitio web de PCI SSC.

Dispositivos ID Tech:

Las versiones de firmware para estos dispositivos solo se pueden ver utilizando una aplicación proporcionada por ID Tech. Para descargar esta aplicación, comuníquese con compliance@freedompay.com para obtener asistencia.

Dispositivos Castles/Elo:

Abra el menú de la aplicación CX desde la pantalla principal, luego haga clic en "Acerca de". En la parte inferior de esta pantalla, verá la versión del firmware.

Dispositivos Ziosk:

La versión del firmware se puede ver en el menú del dispositivo yendo a Configuración > Acerca del dispositivo > Versión del firmware.

Dispositivos Infinite Peripheral:

Las versiones de firmware para estos dispositivos solo se pueden ver utilizando una aplicación proporcionada por Infinite Peripherals. Para descargar esta aplicación, comuníquese con compliance@freedompay.com para obtener asistencia.

Dispositivos PAX:

Desde la pantalla de inicio, seleccione Configuración > Acerca de y registre el firmware mostrado.

Dispositivos Toast:

Desde la pantalla de inicio, seleccione Configuración > Acerca de y registre el firmware mostrado.

Dispositivos Verifone:

Desde la pantalla de inicio, seleccione Configuración > Acerca de y registre el firmware mostrado.

Apéndice A: Solicitud de Exclusión del Comerciante

Esta solicitud de exclusión debe ser firmada por un representante autorizado del comerciante, según lo reflejado en los registros de FreedomPay. Antes de enviar una Solicitud de Exclusión del Comerciante, comuníquese con el Soporte Técnico de FreedomPay para obtener instrucciones sobre el proceso de exclusión. El Soporte Técnico verificará al representante autorizado del comerciante y proporcionará un Número de Incidente.

Número de Incidente (si aplica): _____

Fecha de Solicitud de Exclusión: _____

El comerciante que suscribe la presente solicita optar por salir de la Solución P2PE de FreedomPay. Al firmar esta solicitud, el comerciante reconoce que:

1. Las transacciones procesadas mientras la exclusión esté en efecto no están sujetas a la reducción de alcance de P2PE.
2. El comerciante es el único responsable de implementar controles alternativos para proteger los datos de las cuentas en lugar de la Solución P2PE de FreedomPay.
3. El comerciante está obligado a informar a su adquirente o marca de pago que ha optado por salir de la Solución P2PE de FreedomPay.
4. FREEDOMPAY RENUNCIA A TODAS LAS REPRESENTACIONES Y GARANTÍAS RELACIONADAS CON LA SOLUCIÓN P2PE DE FREEDOMPAY PARA CADA TRANSACCIÓN PROCESADA MIENTRAS LA EXCLUSIÓN ESTÉ EN EFECTO.
5. FREEDOMPAY RENUNCIA A TODA RESPONSABILIDAD, INCLUYENDO, PERO NO LIMITADO A, UNA VIOLACIÓN DE DATOS RESULTANTE DEL PROCESAMIENTO DE PAGOS POR PARTE DEL COMERCIANTE SIN UTILIZAR LA SOLUCIÓN P2PE VALIDADA DE FREEDOMPAY Y LA PLATAFORMA DE COMERCIO DE FREEDOMPAY.

6. El comerciante tiene 60 días desde el momento de la exclusión ("ventana de exclusión") para resolver las condiciones que motivaron la exclusión y volver a inscribirse en la solución, a menos que se acuerde por escrito una ventana de exclusión diferente entre FreedomPay y el comerciante. Después de la ventana de exclusión, el comerciante puede estar restringido de procesar transacciones en la Plataforma de Comercio de FreedomPay de manera indefinida.

Nota: Después de la exclusión, un comerciante puede optar por volver a inscribirse en la Solución de Reducción de Alcance P2PE de FreedomPay, sujeto a los protocolos de seguridad establecidos por FreedomPay, incluyendo una declaración del comerciante que confirme que todos los remanentes de datos de titulares de tarjetas en texto claro han sido eliminados de los sistemas del comerciante utilizando procesos seguros de eliminación de datos.

Comerciante: _____

Firma: _____

(Nombre del Personal Autorizado del Comerciante - Impreso)

Nombre: _____

Título: _____

(Nombre del Personal Autorizado del Comerciante – Firma)

Por favor, envíe este formulario por correo electrónico a: compliance@freedompay.com

Apéndice C: Ejemplos de Identificación de Números de Serie de Dispositivos POI

Las imágenes a continuación muestran algunos ejemplos de dispositivos POI de varios fabricantes y la ubicación física de los números de serie aplicados por las Instalaciones de Inyección de Claves para propósitos de inspección, verificación o RMA (quienes también pueden ayudar con la ubicación o mapeo de números de serie). Para preguntas adicionales relacionadas con los números de serie de dispositivos POI, comuníquese con compliance@freedompay.com.

Ingenico Lane 3000



Quantum Pay Reader 250



Ziosk

