



Manual de instrucciones de P2PE (PIM)
Guía para comerciantes sobre la
implementación y el mantenimiento de la
solución de reducción del ámbito de
aplicación FreedomPay® P2PE

Versión 3.4

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

1.1 Información de la solución P2PE (según el listado en el sitio web de PCI SSC)

Nombre de la solución P2PE:	FreedomPay Commerce Platform P2PE
Número de referencia del listado de la solución P2PE (Asignado por PCI SSC)	2025-00909.016
https://listings.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions	

1.2 Información de contacto del proveedor de la solución P2PE

Nombre de la empresa:	FreedomPay, Inc.		URL de la empresa:	http://corporate.freedompay.com		
Nombre del contacto:	Bernard Clary		Puesto :	VP de Cumplimiento		
Teléfono:	+1-610-902-9000		Correo electrónico:	compliance@freedompay.com		
Domicilio comercial:	FMC Tower at Cira Centre South 2929 Walnut Street · Piso 14		Ciudad:	Philadelphia		
Estado/Provincia:	Pennsylvania	País:	EE. UU.		Código postal:	19104

1.3 Instrucciones de comunicación

Instrucciones sobre cómo comunicarse con el proveedor de la solución P2PE, considerando el establecimiento de un canal/sesión de comunicación confiable.

[Los comercios pueden comunicarse con su Gerente de Éxito del Cliente \(CSM\) asignado, o escribir a \[accounts@freedompay.com\]\(mailto:accounts@freedompay.com\) si no cuentan con un CSM asignado, para preguntas generales relacionadas con su cuenta o implementación.](#)

[Las preguntas de soporte técnico pueden dirigirse a \[techsupport@freedompay.com\]\(mailto:techsupport@freedompay.com\) o mediante el formulario de soporte en nuestra página web.](#)

[Las preguntas de cumplimiento pueden dirigirse a \[compliance@freedompay.com\]\(mailto:compliance@freedompay.com\).](#)

PCI P2PE y PCI DSS

Es posible que los comercios que utilicen esta solución P2PE deban validar su cumplimiento con PCI DSS. Los comercios deben comunicarse con su adquirente o con las marcas de pago para determinar sus requisitos de validación de PCI DSS.

Consulte la [FAQ 1158](#) en el sitio web de PCI SSC.

2. Información del dispositivo PTS POI y del software

2.1 Detalles del dispositivo PTS POI

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

Toda la información de los dispositivos PTS POI puede verificarse visitando lo siguiente en el sitio web de PCI SSC y consultando la Tabla 2.4 a continuación:

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

https://listings.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions

Para las aplicaciones P2PE y el software que no es de pago, utilice los números de ID de PIM para hacer referencia cruzada a sus respectivas tablas a continuación. Los 'números de ID de PIM' son números creados y utilizados por el proveedor de la solución P2PE únicamente para los fines de este PIM, a fin de facilitar la referencia cruzada de las aplicaciones P2PE y el software que no es de pago que se utilizan en los dispositivos PTS POI aquí indicados. Los 'números de ID de PIM' no son asignados por PCI SSC ni son reconocidos por el programa PCI P2PE.

N.º de aprobación PCI PTS	PTS POI Proveedor del dispositivo	Nombre y número(s) de modelo del dispositivo PTS POI	Hardware del dispositivo PTS POI N.º(s) de versión	Firmware del dispositivo PTS POI N.º(s) de versión	Aplicaciones P2PE en dispositivos PTS POI (ID de PIM de la Tabla 2.2)	Software que no es de pago en dispositivos PTS POI (ID de PIM de la Tabla 2.3)
4-20324	Ingenico	Lane/5000	LAN51BA (un cabezal MSR), LAN51CA (doble cabezal MSR), LAN51DA (un cabezal MSR y cámara), LAN51EA (doble cabezal MSR y cámara)	820547v01.xx, 820376v01.xx, 820549v01.xx (SRED OnGuard FPE), 820556v01.xx (SRED OnGuard SDE), 820559v01.xx (SRED ANL), 820555v01.xx (SRED AWL)	App#1, App#2, App#3	NA
4-30257	Ingenico	Lane/8000	LAN80AA, LAN80BA	820547v01.xx	App#1, App#2	NA

4-30326	Ingenico	Link/2500	LIN25AA (versión básica sin compatibilidad con CTLS), LIN25BA (versión básica con CTLS), LIN25CA (versión Companion sin compatibilidad con CTLS), LIN25DA (versión Companion con CTLS), LIN25EA (versión táctil sin compatibilidad con CTLS), LIN25FA (versión táctil con CTLS), LIN25GA (versión de doble cabezal sin compatibilidad con CTLS), LIN25HA (versión de doble cabezal con CTLS), LIN25IA (versión Companion con conector trasero y sin compatibilidad con CTLS), LIN25JA (versión Companion con conector trasero y con CTLS)	820547v01.xx	App#1, App#3	NA
4-30237	Ingenico	Lane/7000	LAN70AA, LAN70AB, LAN70BB	820547v01.xx, 820376v04.xx (Servicios de seguridad)	App#1, App#2	NA

4-20316	Ingenico	Move/5000	<p>MOV50AC (sin CTLS)</p> <p>MOV50AQ (sin CTLS)</p> <p>MOV50AS (sin CTLS)</p> <p>MOV50BB (CTLS)</p> <p>MOV50BC (CTLS)</p> <p>MOV50BQ (CTLS)</p> <p>MOV50BR (CTLS);</p> <p>MOV50DR (CTLS + protector de privacidad);</p> <p>MOV50JR (CTLS + protector de privacidad + tapa de carcasa de escritorio);</p> <p>MOV50BE (CTLS);</p> <p>MOV50DE (CTLS + protector de privacidad);</p> <p>MOV50JE (CTLS + protector de privacidad + tapa de carcasa de escritorio)</p> <p>MOV50BS (CTLS)</p> <p>MOV50CB (sin CTLS + protector de privacidad)</p> <p>MOV50CC (sin CTLS + protector de privacidad)</p> <p>MOV50CQ (sin CTLS + protector de privacidad)</p> <p>MOV50CS (sin CTLS + protector de privacidad)</p> <p>MOV50DB (CTLS + protector de privacidad)</p> <p>MOV50DC (CTLS + protector de privacidad)</p> <p>MOV50DN (CTLS + protector de privacidad)</p> <p>MOV50DQ (CTLS + protector de privacidad)</p> <p>MOV50DS (CTLS + protector de privacidad)</p> <p>MOV50JB (CTLS + protector de privacidad + tapa de carcasa de escritorio)</p>	<p>820376v01.xx,</p> <p>820547v01.xx,</p> <p>820549v01.xx (SRED OnGuard FPE),</p> <p>820555v01.xx (SRED),</p> <p>820556v01.xx (SRED OnGuard SDE),</p> <p>820559v01.xx (SRED ANL),</p> <p>820565v01.xx (SRED FF1)</p>	App#1, App#2, App#3, App#5	NA
---------	----------	---------------------------	--	--	--	--------------------

			<p>MOV50JC (CTLS + protector de privacidad + tapa de carcasa de escritorio)</p> <p>MOV50JN (CTLS + protector de privacidad + tapa de carcasa de escritorio)</p> <p>MOV50JQ (CTLS + protector de privacidad + tapa de carcasa de escritorio)</p> <p>MOV50JS (CTLS + protector de privacidad + tapa de carcasa de escritorio)</p> <p>MOV50AB (sin CTLS)</p> <p>MOV50BN (CTLS)</p>			
4-30310	Ingenico	<i>Lane/3000</i>	<p>LAN30AA, LAN30BA, LAN30CA, LAN30DA, LAN30EA, LAN30FA, LAN30GA, LAN30HA</p>	<p>820547v01.xx, 820561v01.xx (firmware base)</p>	<i>App#1, App#2, App#3</i>	<i>NA</i>
4-20317	Ingenico	<i>DESK/5000</i>	<p>(CTLS) (sin CTLS + protector de privacidad) (sin CTLS) DES50AB, DES50BB, DES50CB, DES50DB (CTLS + protector de privacidad)</p>	<p>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)</p>	<i>App#6</i>	<i>NA</i>
4-30365	Ingenico	<i>Moby/5500</i>	<p>MOB55xBxAx, MOB55ABBBx (con CTLS)</p> <p>MOB55BBABx (sin CTLS)</p> <p>MOB55BBBBx (con CTLS)</p> <p>MOB55ABABx (sin CTLS)</p> <p>MOB55xBxAx</p>	<p>CTRL: xxxx-F-802-01xx-xxxx-xx</p> <p>BOOT: xxxx-F-801-01xx-xxxx-xx</p> <p>CTRL: xxxx-F-802-02xx-xxxx-xx BOOT: xxxx-F-801-02xx-xxxx-xx</p>	NA	NA

4-90307	Ingenico	<i>Moby/5500 CL3</i>	MOB55ABHAX (con CTLS) MOB55BBGAX (sin CTLS) MOB55BBHAX (con CTLS) MOB55ABGAX (sin CTLS)	BOOT: xxxx-F-D01-01xx-xxxx-xx CTRL: xxxx-F-D02-01xx-xxxx-xx USER: xxxx-F-023-02xx-xxxx-xx		NA
4-30263	Ingenico	<i>Moby/8500</i>	MOB85AAx (sin CTLS), MOB85ABx (sin CTLS), MOB85ACx (sin CTLS), MOB85BAx (con CTLS), MOB85BBx (con CTLS), MOB85BCx (con 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	NA	NA
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)	App#2	<i>NA</i>
4-30381	Ingenico	<i>Self/2000</i>	SEL20AA	820376v04.xx (Servicios de seguridad) 820566v01.xx	App#2	<i>NA</i>
4-30393	Ingenico	<i>Self/4000</i>	SEL40BA	820376v04.xx (Servicios de seguridad) 820547v01.xx	App#2	<i>NA</i>
4-30384	Ingenico	<i>Self/5000</i>	SEL50CA	820376v04.xx (Servicios de seguridad) 820566v01.xx	App#2	<i>NA</i>

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)	App#2	<i>NA</i>
4-30535	Ingenico	<i>Self/4000 LE</i>	SEL41AA1-xxxx SEL41AA2-xxxx	820571v01.xx (firmware principal), 820376v12.xx (Servicios de seguridad), 820556v01.xx (SRED On-Guard SDE), 820549v01.xx (SRED On-Guard FPE)	App#2	<i>NA</i>
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)	App#2	<i>NA</i>

4-20359	Ingenico	Move/5000	MOV50BE (CTLS) MOV50BQ (CTLS) MOV50BR (CTLS) MOV50BS (CTLS) MOV50DC (CTLS + protector de privacidad) MOV50DE (CTLS + protector de privacidad) MOV50DN (CTLS + protector de privacidad) MOV50DQ (CTLS + protector de privacidad) MOV50DR (CTLS + protector de privacidad) MOV50DS (CTLS + protector de privacidad) MOV50JC (CTLS + tapa de carcasa de escritorio) MOV50JE (CTLS + tapa de carcasa de escritorio) MOV50JN (CTLS + protector de privacidad + tapa de carcasa de escritorio) MOV50JQ (CTLS + tapa de carcasa de escritorio) MOV50JR (CTLS + tapa de carcasa de escritorio) MOV50JS (CTLS + tapa de carcasa de escritorio) MOV50BC (CTLS) MOV50BN (CTLS)	820547v11.xx, 820549v01.xx (SRED OnGuard FPE), 820556v01.xx (SRED OnGuard SDE), 820547v11.xx (firmware principal), 820376v12.xx (Servicios de seguridad)	App#1, App#2, App#3, App#5, App#6	NA
---------	----------	---------------------------	--	--	---	----

4-30494	Ingenico	Lane/7000	LAN70AC LAN70BB LAN70BC LAN70BD LAN70AB	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)	App#2	NA
4-30493	Ingenico	Lane/8000	LAN80BA LAN80BB LAN80AA	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)	App#2	NA
4-20375	Ingenico	Lane/5000	LAN52BA1-xxxx	820571v01.xx (firmware principal) 820376v12.xx (Servicios de seguridad) 820549v01.xx (SRED OnGuard FPE) 820556v01.xx (SRED OnGuard SDE) 820376v14.xx (Servicios de seguridad)	App#2, App#3, App#5	NA

4-30533	Ingenico	<i>Link/2500 LE</i>	LIN25AB1-xxxx LIN25BA1-xxxx LIN25CA1-xxxx LIN25DA1-xxxx LIN25AA1-xxxx	820571v01.xx (firmware principal) 820376v12.xx (Servicios de seguridad) 820556v01.xx (SRED On-Guard SDE) 820549v01.xx (SRED On-Guard FPE) 820565v01.xx (SRED FF1) 820376v14.xx (Servicios de seguridad)	<i>App#2</i>	<i>NA</i>
4-30498	Ingenico	<i>AXIUM RX7000</i>	R70411xxxx	02.03.11.xxxxx (La solución SRED compatible con el firmware incluye SRED EP2, SRED C-TAP, SRED ZVT-H, SRED OnGuard FPE, SRED OnGuard SDE, SRED FF1)	<i>App#4</i>	<i>SW#1</i>
4-30444	Ingenico	<i>AXIUM EX8000</i>	E801x2	01.09.11.xxxxx (con AP Solution 1, SRED EP2, SRED C-TAP, SRED ZVT-H, SRED OnGuard SDE, SRED OnGuard FPE, SRED FF1)	<i>App#4</i>	<i>SW#1</i>
4-30443	Ingenico	<i>AXIUM DX8000-2, AXIUM DX8000-5</i>	D851x3 (con AP Solution 1)	01.09.11.xxxxx (con AP Solution 1 SRED EP2 SRED C-TAP SRED ZVT-H SRED OnGuard SDE SRED OnGuard FPE SRED FF1)	<i>App#4</i>	<i>SW#1</i>
4-30527	Ingenico	<i>AXIUM RX5000</i>	R50411xxxx (sin protector de PIN)	02.03.11.xxxxx (La solución SRED compatible con el firmware incluye: SRED EP2 SRED C-TAP SRED ZVT-H SRED OnGuard SDE SRED OnGuard FPE SRED FF1)	<i>App#4</i>	<i>SW#1</i>
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	<i>NA</i>	<i>NA</i>

4-90385	ID Tech	SREDKey2	80172002 (sin MSR) 80172004 (con MSR) 80172005 (sin MSR) 80172007 (sin MSR) 80172001 (con MSR) 80172006 (con MSR)	SREDKEY2 FW v1.03.xxx.xxx.S SREDKEY2 FW v2.01.xxx.xxx.S	NA	
4-30432	Infinite Peripherals, Inc	QuantumPay Reader 250	06.00.xx.xx	3.0.xx.xx	NA	NA
4-30433	Infinite Peripherals, Inc	QuantumPay Reader 300	05.11.xx.xx	3.1.xx.xx, 3.2.xx.xx	NA	NA
4-30437	Infinite Peripherals, Inc	QuantumPay PIN 400	00xxxD1xxxxxx (versión sin CTLS) CLxxxD1xxxxxx (versión con CTLS)	3.1.xx.xx, 3.2.xx.xx	NA	NA
4-30438	Infinite Peripherals, Inc	QuantumPay Connected 150	PRR05xxx PRR15xxx PXR05xxx PXR15xxx	3.0.xx.xx, 3.1.xx.xx	NA	NA
4-30511	Infinite Peripherals, Inc	QuantumPay Connected 250 and 252	51DxxxxNxxxx versión sin CTLS 51DxxxxCxxxx versión con CTLS	3.0.xx.xx	NA	NA
4-30453	Infinite Peripherals, Inc	QuantumPay PIN 401	41D1xxxN0xxx 41D1xxxC0xxx	3.0.xx.xx	NA	NA
4-30464	Infinite Peripheral, Inc	QuantumPay PIN 451	41D1xxxN1xxx - versión sin CTLS 41D1xxxC1xxx - versión con CTLS	3.0.xx.xx	NA	NA

4-30318	Datacs Ltd.	<i>BluePad-5000 (QuantumPay PIN 600)</i>	02.05.2x.0xxxxa (BluePad-5000 v2) 02.05.2x.1xxxxa (BluePad-5000 v2) 02.05.2x.2xxxxa (BluePad-5000 v2) 02.05.3x.0xxxxa (BluePad-5000 v3) 02.05.3x.1xxxxa (BluePad-5000 v3) 02.05.3x.1xxxxx (BluePad-5000 v3) 02.05.3x.2xxxxa (BluePad-5000 v3) 02.05.3x.xxxxxa (BluePad-5000 v3) 02.05.4x.0xxxxa (BluePad-5000 v4) 02.05.4x.1xxxxa (BluePad-5000 v4) 02.05.4x.1xxxxx (BluePad-5000 v4) 02.05.4x.2xxxxa (BluePad-5000 v4) 02.05.4x.xxxxxa (BluePad-5000 v4) 02.05.5x.0xxxxa (BluePad-5000 v5) 02.05.5x.1xxxxa (BluePad-5000 v5) 02.05.5x.1xxxxx (BluePad-5000 v5) 02.05.5x.2xxxxa (BluePad-5000 v5) 02.05.5x.xxxxxa (BluePad-5000 v5) 02.05.2x.1xxxxx (BluePad-5000 v2) 02.05.2x.xxxxxa (BluePad-5000 v2)	3.2.xx.xx 3.1.xx.xx	NA	NA
---------	-------------	--	--	------------------------	----	----

4-30475	Infinite Peripherals, Inc	<i>QuantumPay Pro Plus</i>	21.1x.xx.xxx	SP: 3.0.xx.xx, AP: 1.0.xx.xx	NA	NA
4-80037	Castles Technology Co. Ltd	<i>Saturn 1000-E</i>	SATURN1000E-HW- V1.20.xxxx	1.1.1.xxxxxx	NA	<i>SW#1-22</i>
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	NA	<i>SW#1-22</i>
4-30416	Castles Technology Co. Ltd	<i>Saturn 1000</i>	SATURN1000-HW- V2.00.xxxx	1.3.1.xxxxxx 1.4.1.xxxxxx	NA	<i>SW#1-22</i>
4-80075	Castles Technology Co. Ltd	<i>S1E2, S1E2-L, S1E2N</i>	HW-V1.00, S1E2: HW- V1.00	S1E2 & S1E2-L:	NA	<i>SW#1-22</i>
4-80094	Castles Technology Co. Ltd	<i>S1F4 PRO</i>	HW-V-1G.00	1.6.1.xxxxxx	NA	<i>SW#1-22</i>
4-80082	Castles Technology Co. Ltd	<i>S1P</i>	HW-V1.00	1.4.1.xxxxxx	NA	<i>SW#1-22</i>
4-80092	Castles Technology Co. Ltd	<i>S1P2</i>	HW-V-1D.00	1.6.1.xxxxxx	NA	<i>SW#1-22</i>
4-80091	Castles Technology Co. Ltd	<i>S1Mini2</i>	HW-V-1E.00	1.6.1.xxxxxx	NA	<i>SW#1-22</i>
4-80118	Castles Technology Co. Ltd	<i>S1E4 PRO</i>	HW-V-1P.00	1.6.1.xxxxxx 13.0002.xxxx.xxxx.xxxx_xx xx.xxxx.xxxx	NA	<i>SW#1-22</i>
4-80106	Castles Technology Co. Ltd	<i>S1U2-M4</i>	HW-V-1I.00	1.6.1.xxxxxx	NA	<i>SW#1-22</i>

4-80084	Castles Technology Co. Ltd	S2L	HW-V1A.00	1.4.1.xxxxxx	NA	SW#1-22
4-80077	Castles Technology Co. Ltd	S1U2	HW-V1.00	1.4.1.xxxxxx 1.4.2.xxxxxx	NA	SW#1-22
4-30470	Elo Touch Solutions, Inc	EMC0600, EMC0600C, EMC0600SC' EMC0600S	A01.0EC.x A01.0NC.x A01.S00.x A01.SEC.x A01.SNC.x A01.000.x	5.xxx.xxx.xxxx+ap 5.xxx.xxx.xxxx+p 6.xxx.xxx.xxxx+ap 6.xxx.xxx.xxxx+p	NA	NA
4-90136	Ziosk	Z600	6.0.A 6.0.B	6201.29.xxxx.xxx.xxx 6201.30.xx.x.xxx	NA	NA
4-90335	Ziosk	Z600 Pro	6.0.A	6201.29.xxxx.xxx.xxx	NA	NA
4-30522	Verifone	M425 M450	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	NA	NA
4-80062	Verifone	P630	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	NA	NA

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	NA	<i>NA</i>
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	NA	<i>NA</i>
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	NA	<i>NA</i>
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	NA	<i>NA</i>
4-30554	Toast Inc	<i>TG300, TG310</i>	REV1.xx	01.xx.xx.-10xxxxx	NA	<i>SW#1</i>

2.2 Detalles de las aplicaciones P2PE

La siguiente información enumera las aplicaciones P2PE aprobadas para su uso en los dispositivos PTS POI de la Tabla 2.1 para esta solución P2PE.

Por definición, las aplicaciones P2PE tienen acceso a datos de cuenta en texto claro. Estas aplicaciones **deben** estar indicadas en el listado de la solución P2PE.

Los 'números de ID de PIM' son números creados y utilizados por el proveedor de la solución P2PE únicamente para los fines de este PIM, a fin de facilitar la referencia cruzada de las aplicaciones P2PE aquí indicadas que se utilizan en los dispositivos PTS POI indicados en la Tabla 2.1. No son asignados por PCI SSC ni son reconocidos por el programa PCI P2PE.

Nota: Las aplicaciones P2PE que se evaluaron como parte de la solución P2PE y que se eligió no listar por separado se indican como tales en el listado de la solución P2PE y no tendrán un número de referencia de listado de aplicación PCI P2PE independiente.

https://listings.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions

ID de PIM (p. ej., App#1, App#2, ...)	Proveedor de la aplicación P2PE	Nombre de la aplicación P2PE	Versión(es) de la aplicación P2PE	Número de referencia del listado de la aplicación PCI P2PE (Asignado por PCI SSC)
App#1	Ingenico	UPP	1.1.x	2023-00470.045
App#2	Ingenico	UPP	2.0.x	2023-00470.051
App#3	Ingenico	RA1	20.x	2024-00470.056
App#4	Ingenico	Axiom Retail Core Axiom Payment Service (ARC APS)	1.0.x	2024-00470.059
App#5	Ingenico	IngeProtect	2.1.x.x.x	2025-01079.009
App#6	FreedomPay	Aplicación independiente FreeWay (FSA)	3.0.x	2025-00909.015

2.3 Detalles del software que no es de pago

La siguiente información enumera el software que no es de pago aprobado para su uso en los dispositivos PTS POI de la Tabla 2.1 para esta solución P2PE.

*Por definición, el software que no es de pago de P2PE **no debe** tener acceso alguno a datos de cuenta en texto claro. Si bien este tipo de software se evalúa como parte de la evaluación de la solución P2PE, no se indica en el listado de soluciones PCI P2PE.*

Los 'números de ID de PIM' son números creados y utilizados por el proveedor de la solución P2PE únicamente para los fines de este PIM, a fin de facilitar la referencia cruzada del software que no es de pago aquí indicado que se utiliza en los dispositivos PTS POI indicados en la Tabla 2.1. No son asignados por PCI SSC ni son reconocidos por el programa PCI P2PE.

ID de PIM (p. ej., SW#1, SW#2, ...)	Proveedor del software que no es de pago	Nombre del software que no es de pago	Versión(es) del software que no es de pago	Información adicional (según sea necesario)
SW#1	FreedomPay	CX App	1.x.x	Componente de middleware de Android para integrarse con aplicaciones de POS en dispositivos todo en uno
SW#2	MyVenue	mvPOS	2.71, 3.38	
SW#3	Tapin2	Tapin2 Web View App	2x.xx.xxx	
SW#4	Agilysys	rGuestPay	2x.xx.xxx	
SW#5	Up'n'Go	UpNGoPay	1.x.x	
SW#6	Agilysys	IG FLY	12.3.x.x	
SW#7	RetailCloud	6IX POS	3.x.x	
SW#8	HotelKey	RK Register	5.02, 6.01	
SW#9	Verteda	SwiftPOS	4.x	
SW#10	Zonal	iServe	2.x.x.x	
SW#11	Kappture	Kappture epos	1.10.x.x	
SW#12	OTG	Skywire Pay	1.0.2	
SW#13	RetailCloud	Inventory360	2.3.3	
SW#14	Tevalis	TevX	20xx.xx.xx	

2.3 Detalles del software que no es de pago

SW#15	OutPay	OutPay FOH	1.x.x	
SW#16	Shiji	Infrasys	1.x.x	
SW#17	Axess	RetailPOS	3.0.0	
SW#18	Campana AXIS	FPConnector	1.0.7	
SW#19	Haven	SandCastles Pay	1.0.0	
SW#20	SmartQ	Time2Eat MPOS	1.08	
SW#21	OTG	floServe	1.0.7, 2.3.0	
SW#22	OTG	SkyWire Companion	0.1.3	

2.4 Verificación de la información del dispositivo PTS POI

Verificar la información del dispositivo PTS POI es fundamental. Esta información es necesaria para validar la información de este PIM, para realizar referencias cruzadas con los listados de PCI PTS y con el listado de soluciones PCI P2PE, además de para la administración de inventario, la resolución de problemas y el reporte de incidentes.

Instrucciones para confirmar el hardware, el firmware del dispositivo PTS POI y las aplicaciones P2PE y el software que no es de pago presentes

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

Dispositivos Ingenico:

Para encontrar la versión del firmware, siga estos pasos:

1. Desconecte el dispositivo del sistema POS o de otro sistema de front-end
2. Alimente el dispositivo con el cable de corriente o conectándolo a una PC mediante el cable USB
3. Durante el arranque 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 de teclas sería 2634, [botón verde], +
5. Si utiliza un Move/5000, use el código 0001
6. Seleccione el siguiente menú: *Control Panel/Terminal Information/Firmware PCI PTS/Display*

7. 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 "PCI Version" debe coincidir con la plantilla de número de versión que se muestra en el sitio web de PCI SSC.

Dispositivos ID Tech:

Las versiones de firmware de estos dispositivos solo se pueden ver mediante 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 y luego haga clic en "About". 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, en Settings > About device > Firmware version.

Dispositivos Infinite Peripheral:

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

Dispositivos PAX

En la pantalla de inicio, seleccione Settings > About y registre el firmware que se muestra.

Dispositivos Toast

En la pantalla de inicio, seleccione Settings > About y registre el firmware que se muestra.

Dispositivos Verifone

En la pantalla de inicio, seleccione Settings > About y registre el firmware que se muestra.

2.5 Inventario y monitoreo de dispositivos PTS POI

- Todos los dispositivos PTS POI deben documentarse mediante procedimientos de control de inventario y monitoreo, incluido el estado del dispositivo (p. ej., implementado, en espera de implementación, en reparación o de otro modo fuera de uso, o en tránsito).
- Este inventario debe realizarse, como mínimo, una vez al año.
- Cualquier discrepancia en el inventario, incluidos los dispositivos PTS POI faltantes o sustituidos, debe reportarse a el proveedor de la solución P2PE mediante la información de contacto y las instrucciones de la Sección 1 anterior.
- La siguiente tabla de inventario de muestra es solo con fines ilustrativos. El comercio debe capturar y mantener el inventario real en un documento externo.

Instrucciones para documentar y mantener un inventario de los dispositivos PTS POI.

El comercio debe implementar y mantener un sistema de seguimiento de dispositivos POI que identifique cada dispositivo POI según su estado actual. Algunos ejemplos de posibles estados son:

- Implementado
- En espera de implementación
- Fuera de servicio y/o en reparación
- En tránsito
- Retirado y devuelto

FreedomPay ofrece un sistema básico de registro a través de su Enterprise Reporting Portal, denominado Device Management Portal, que puede configurarse durante la implementación. Como alternativa, los comercios pueden implementar su propio sistema si lo prefieren. Los inventarios electrónicos de dispositivos POI deben almacenarse de forma segura, con acceso limitado únicamente al personal autorizado.

El comercio también debe establecer un “sistema estatal de contabilidad y control” para llevar el registro de todos los dispositivos POI (cantidad y tipo), registrar los cambios en los inventarios de materiales (entradas/salidas) y monitorear todos los aspectos del ciclo de vida del dispositivo POI mientras este se encuentre en posesión y bajo el control del comercio. Registre todas las discrepancias de inventario en su sistema de control de inventario y reporte a FreedomPay los dispositivos faltantes o extraviados una vez identificados, a compliance@freedompay.com, o al socio/revendedor designado de FreedomPay que proporcionó los dispositivos.

Si su organización cuenta con múltiples tiendas, es regional u opera a nivel nacional, es importante emplear sistemas de administración y seguimiento de inventario en los niveles local, regional y nacional para asegurar que el conocimiento y la capacidad para administrar, dar seguimiento y reportar los inventarios se cumplan 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 necesaria para el seguimiento del inventario se puede encontrar en una etiqueta en el panel posterior o en el compartimento de la batería de cada dispositivo POI (las imágenes de la ubicación del número de serie de una muestra de dispositivos se incluyen en el **Apéndice C de la Sección 9, Orientación adicional** y/o mediante la interfaz lógica del dispositivo POI.)

El comercio debe desarrollar y mantener protocolos escritos para la reubicación de dispositivos entre las ubicaciones del comercio. El comercio debe monitorear y documentar el cumplimiento de dichos protocolos. Los protocolos de reubicación de dispositivos POI del comercio deben ser, como mínimo, 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 durante la reubicación o el almacenamiento de dispositivos, comuníquese con compliance@freedompay.com o con el socio/revendedor de FreedomPay que proporcionó los dispositivos.

Es posible que se solicite al comercio presentar su inventario anual de POI a su adquirente como parte de su cumplimiento anual con PCI DSS. No seguir los controles enumerados en el PIM puede dar lugar a la “Exclusión del comercio” (Merchant Opt-Out), es decir, la suspensión del programa de reducción del alcance FreedomPay Commerce Platform P2PE.

Si un comercio ya no desea utilizar los dispositivos POI proporcionados por FreedomPay como parte de un programa de reducción del alcance PCI P2PE debido a una exclusión del comercio, terminación del contrato, cierre del negocio, baja de operaciones u otro motivo, el comercio debe destruir de forma segura todos los dispositivos POI proporcionados por FreedomPay. La destrucción segura debe realizarse mediante el servicio de destrucción segura de FreedomPay, enviando una solicitud a devicedisposal@freedompay.com indicando el número de dispositivos y los números de serie de cada uno. Una vez recibida, el equipo de Professional Services de FreedomPay responderá con más detalles. Para obtener más información sobre posibles servicios de destrucción, comuníquese con su representante de FreedomPay.

Tabla de inventario de muestra

Proveedor del dispositivo PTS POI	Nombre(s) y número(s) de modelo del dispositivo PTS POI	Ubicación del dispositivo	Estado del dispositivo	Número de serie u otro identificador único	Fecha del inventario	Notas adicionales (según sea necesario)

3. Recepción de dispositivos PTS POI

3.1 Instrucciones para asegurar que los dispositivos PTS POI provengan de fuentes/sitios/ubicaciones confiables

FreedomPay o su KIF certificado enviará por correo electrónico al comercio una notificación previa al envío que identifica los números de serie de los dispositivos POI, el nombre de la empresa de mensajería, el número de rastreo, la instalación desde la cual se envió el paquete y la ubicación aprobada del comercio a la que se envió el paquete.

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

- i. Inspeccionar el empaque como se indicó anteriormente.
- ii. Verificar que la empresa de mensajería identificada en el acuse de entrega sea una empresa de mensajería de confianza (Trusted Courier).
- iii. Verificar que el paquete haya sido enviado desde una instalación de proveedor asociada con uno o más proveedores de componentes incluidos en FreedomPay's Commerce Platform P2PE, o desde una instalación que forme parte de la cadena de custodia preestablecida del comercio. Si no está seguro de la dirección o ubicación de la cual debería provenir un dispositivo, comuníquese con compliance@freedompay.com.
- iv. Verificar que los números de serie del comprobante de envío coincidan con los números de serie del correo electrónico de notificación previa al envío.
- v. Actualizar el sistema de registro de dispositivos para reflejar el cambio en el estado y la ubicación del dispositivo.

El comercio debe devolver de inmediato a FreedomPay, según se indica a continuación, cualquier paquete de dispositivos POI que parezca haber sido manipulado, que haya sido entregado por alguien que no sea una empresa de mensajería de confianza o que haya sido enviado desde una ubicación distinta de una instalación esperada.

Antes de devolver un dispositivo POI a una instalación de proveedor aprobado, el comercio debe enviar un correo electrónico a poidevicereturns@freedompay.com para determinar a dónde debe enviarse el dispositivo según la situación.

3.2 Instrucciones para confirmar que el dispositivo PTS POI y su empaque no fueron manipulados

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

- Verificar la empresa de mensajería identificada en el acuse de entrega
- Verificar que el paquete haya sido enviado desde una instalación esperada.
- Verificar que los números de serie del comprobante de envío coincidan con los números de serie del correo electrónico de notificación previa al envío.
- Verificar que el empaque no esté dañado al grado de exponer el interior del paquete.
- Verificar que el empaque no se haya mojado al grado de que la humedad haya penetrado las paredes del empaque.

- Verificar que la integridad del empaque con sello de seguridad contra manipulación esté intacta.

Ejemplo de un paquete sin manipular con cinta de seguridad contra manipulación:



Si el dispositivo o el empaque no superan alguna de las inspecciones anteriores, comuníquese con su representante de FreedomPay y devuelva el dispositivo como se describe en la Sección 5.2.

3.3 Instrucciones para confirmar la necesidad comercial y la identidad de cualquier personal externo que afirme ser personal de entrega, soporte y/o reparación, antes de otorgarle acceso a los dispositivos PTS POI.

En la mayoría de los casos, FreedomPay podrá brindar soporte a los dispositivos de forma remota, sin necesidad de asistencia en sitio. Sin embargo, durante instalaciones complejas o en ciertos casos de soporte, es posible que se envíe a un técnico a la ubicación del comercio. Si se requiere un técnico de FreedomPay en sitio, asegúrese de seguir los siguientes pasos antes, durante y después de que se realice el trabajo en sitio.

- Se asignará un técnico de campo al caso y se completará una solicitud de despacho.
- Una vez asignado el técnico, FreedomPay proporcionará al comercio los detalles de la solicitud.
- Cuando el técnico llegue al sitio, y antes de permitirle el acceso al dispositivo POI, el comercio debe verificar la identidad del técnico como empleado o contratista de FreedomPay. Se debe negar el acceso a cualquier otro personal que no valide adecuadamente su identidad.
- Una vez verificada la identidad del técnico, el comercio debe asignar a un acompañante para supervisar la actividad del técnico en todo momento.
- Una vez que el técnico haya terminado el trabajo, el comercio debe responder al correo electrónico de despacho con los siguientes detalles:

- i. Tipo de identificación presentada para la verificación
- ii. Tiempo que permaneció en la ubicación
- iii. (Solo para casos de soporte) Número(s) de serie de la(s) terminal(es) que el técnico intervino

FreedomPay nunca enviará técnicos al sitio sin coordinarse previamente con los contactos del comercio y proporcionar información sobre el técnico que se envía para fines de verificación. No se debe permitir el acceso a los dispositivos POI a nadie que afirme ser técnico de reparación/soporte sin la notificación o identificación adecuadas.

Proteja físicamente los dispositivos POI que se encuentren en su posesión, incluidos los dispositivos:

- En espera de implementación
- En reparación o de otro modo fuera de uso
- En espera de transporte entre sitios/ubicaciones

4. Implementación e instalación de dispositivos PTS POI

No conecte ni utilice de otro modo dispositivos de captura de datos de cuentas de pago no aprobados.

La solución P2PE está aprobada para utilizar dispositivos PTS POI específicos, como se detalla anteriormente en la Tabla 2.1, los cuales deben estar indicados en el listado de la solución P2PE.

Si se utiliza algún dispositivo que no esté en la Tabla 2.1 para aceptar datos de cuentas de pago, podría afectar la elegibilidad del comercio para utilizar el SAQ P2PE; comuníquese con su adquirente o con las marcas de pago.

No cambie ni intente cambiar las configuraciones o los ajustes seguros del dispositivo PTS POI.

Cambiar las configuraciones o los ajustes seguros del dispositivo PTS POI puede invalidar la implementación de la solución P2PE y podría afectar la elegibilidad del comercio para utilizar el SAQ P2PE; comuníquese con su adquirente o con las marcas de pago.

Algunos ejemplos, entre otros, son intentar realizar lo siguiente en los dispositivos PTS POI:

- Habilitar cualquier interfaz del dispositivo o mecanismo de captura de datos que esté deshabilitado
- Alterar las configuraciones de seguridad o los controles de autenticación
- Abrir físicamente el dispositivo
- Intentar instalar aplicaciones/software no autorizados

4.1 Instrucciones de instalación y conexión de los dispositivos PTS POI

Se recomienda proteger la instalación de cada dispositivo POI mediante uno de los siguientes métodos o una alternativa aprobada por su Asesor de Seguridad Calificado (QSA):

- i. El dispositivo está montado o sujeto físicamente para evitar su retiro, manipulación o sustitución no autorizados. Los métodos aceptables incluyen:
 - a. Montar el dispositivo en un soporte de seguridad para PIN aprobado
 - b. Asegurar el dispositivo mediante un cable con candado conectado a la ranura de seguridad del dispositivo POI y fijado de manera permanente al mostrador o a otro hardware seguro fijado físicamente en el extremo opuesto del cable. Hay una amplia variedad de cables con candado disponibles en la mayoría de las tiendas de computadoras, en línea o a través de FreedomPay. Comuníquese con su representante de FreedomPay si necesita ayuda para encontrar un cable con candado adecuado.
- ii. El dispositivo debe ubicarse de modo que el personal autorizado pueda observarlo/monitorearlo fácilmente y en un entorno que disuada los intentos de vulneración.

Los pasos adicionales de implementación incluyen:

- i. Al iniciar el dispositivo, el comercio debe realizar los siguientes pasos:
 - a. Verificar que el número de serie que se muestra coincida con el número de serie en la parte inferior del dispositivo.
 - i. Para obtener ayuda para ubicar los números de serie en los dispositivos POI, consulte el **Apéndice C en la Sección 9, Orientación 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. Serie
 - c. Ethernet
 - d. Wi-Fi
 - e. Bluetooth
 - f. Celular

Otro: Para los tipos de comunicación de POI no incluidos anteriormente, el comercio debe comunicarse con compliance@freedompay.com para recibir la aprobación oficial de cumplimiento de FreedomPay, por parte de su equipo de cumplimiento, para el uso de dicho dispositivo. El comercio debe recibir por escrito una certificación oficial de FreedomPay que indique que el tipo de comunicación de POI, que no figura en la lista anterior, es un método de comunicación/conexión aceptado para la solución FreedomPay Commerce Platform P2PE.

4.2 Orientación para seleccionar ubicaciones adecuadas para implementar los dispositivos PTS POI

FreedomPay recomienda, y PCI DSS refuerza, que todos los dispositivos implementados estén montados de forma segura y sean fácilmente visibles para el personal, a fin de evitar su retiro o manipulación no autorizados. El dispositivo debe ubicarse de modo que el personal autorizado pueda observarlo/monitorearlo fácilmente y en un entorno que disuada los intentos de vulneración. Si una implementación se designa para uso desatendido, deben existir procedimientos para mitigar el riesgo asociado con dicha 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 Orientación para proteger físicamente los dispositivos PTS POI implementados a fin de evitar su retiro y/o sustitución no autorizados

Se recomienda a los comercios montar los dispositivos en servicio en un soporte de seguridad para PIN aprobado o asegurar el dispositivo mediante un cable con candado conectado a la ranura de seguridad del dispositivo POI y fijado de manera permanente en el extremo opuesto del cable. Hay una amplia variedad de cables con candado disponibles en la mayoría de las tiendas de computadoras o en línea. Comuníquese con su representante de FreedomPay o con su QSA si necesita ayuda para encontrar un cable con candado

adecuado. Para implementaciones que no favorecen el uso de dispositivos montados (p. ej., dispositivos independientes o escenarios móviles), deben implementarse procedimientos para mitigar el riesgo de manipulación o vulneración 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 comercio debe establecer un área de “almacenamiento seguro” para los dispositivos POI que no estén en servicio. Este almacenamiento se utilizará cuando se reciban dispositivos POI de FreedomPay antes de su instalación, cuando se transfieran desde otras ubicaciones aprobadas del comercio o cuando se retiren del uso activo. PCI define el almacenamiento seguro como un espacio o ubicación designado con acceso físico controlado, en el que el personal debe estar autorizado para obtener acceso y existen mecanismos/políticas para documentar todo acceso físico al área de “almacenamiento seguro”, incluido:

- Identificar al personal autorizado para acceder a los dispositivos
- Restringir el acceso al personal autorizado
- Mantener un registro de todos los accesos que incluya nombre del personal, empresa, motivo del acceso y hora de entrada y salida

El comercio 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 es y dónde se encuentra el área de almacenamiento seguro, así como los procedimientos establecidos para cumplir con los requisitos establecidos en esta sección.

5. Monitoreo e inspección continuos de los dispositivos PTS POI implementados

5.1 Instrucciones para inspeccionar los dispositivos PTS POI en busca de señales de manipulación y responder ante incidentes de manipulación sospechada

Los comercios deben inspeccionar lo siguiente, como mínimo, en un plazo adecuado según su perfil de riesgo (normalmente de forma trimestral):

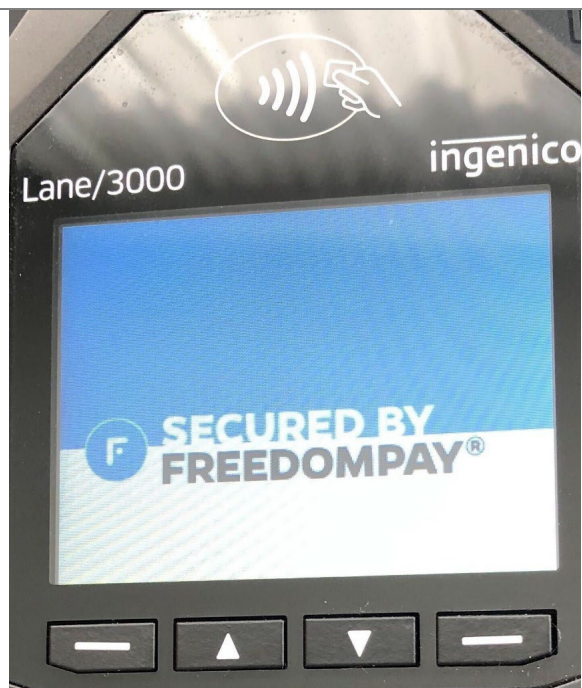
- ¿El cable USB/Ethernet ha sido dañado o alterado de alguna manera?
- ¿El número de serie del dispositivo coincide con el número de serie proporcionado por FreedomPay? (Consulte el Apéndice C para ver la ubicación del número de serie)
- ¿Los dispositivos POI activos están protegidos de manera adecuada conforme al PIM?
- ¿Los dispositivos POI inactivos están almacenados de forma segura conforme al PIM?
- ¿El dispositivo POI ha sido dañado de alguna manera?
- ¿Aparece la pantalla “Secured by FreedomPay”?
- ¿Están intactas las medidas adicionales de detección de manipulación que el comercio haya agregado y registrado en el inventario, como sellos de seguridad, etiquetas o marcas ocultas?

Ejemplos de áreas de inspección:

Verifique que no se hayan retirado los tornillos exteriores.



Verifique que aparezca la pantalla “Secured by FreedomPay”.



Si un comercio implementa un dispositivo POI de FreedomPay en un área que no esté monitoreada físicamente por un empleado aprobado del comercio, deben existir procedimientos adecuados para reducir la posibilidad de manipulación del dispositivo y, en el peor de los casos, el tiempo entre la vulneración y su detección. Consulte a su Asesor de Seguridad Calificado (QSA) independiente para obtener información adicional sobre la inspección y el monitoreo de POI.

Cualquier caso de manipulación de un dispositivo debe reportarse a FreedomPay, y cualquier dispositivo que haya sido manipulado o que se sospeche que lo ha sido debe retirarse de inmediato del entorno POS y devolverse a FreedomPay conforme a las instrucciones descritas en la Sección 5.2.

El comercio debe devolver de inmediato a FreedomPay, según se indica 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 una empresa de mensajería de confianza (Trusted Courier) o que haya sido enviado desde una ubicación distinta de una instalación de proveedor aprobado.

Envío de dispositivos POI:

- i. Los dispositivos POI solo pueden ser transportados por una empresa de mensajería de confianza (Trusted Courier) a una instalación de proveedor aprobado incluida en la sección 4.2.

- ii. Los números de serie de los dispositivos que se devuelven, junto con el motivo de la devolución, deben comunicarse a RMA@freedompay.com quien generará una etiqueta de envío para la devolución.
- iii. Todos los números de serie de los dispositivos POI deben imprimirse en el comprobante de empaque o en la etiqueta de envío.

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

5.2 Instrucciones para inspeccionar los dispositivos PTS POI en busca de dispositivos skimmer y responder ante la detección sospechada de skimming

Puede encontrar orientación adicional para inspeccionar dispositivos PTS POI en el documento titulado *Skimming Prevention: Best Practices for Merchants*, disponible en https://www.pcisecuritystandards.org/document_library/

Revise los puntos de interacción en busca de superposiciones o herramientas insertadas.



Revise el punto de conexión en busca de cables/conexiones o hardware adicionales.



5.3 Instrucciones para detectar y responder ante fallas de cifrado de datos de cuenta en dispositivos PTS POI

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

- i. Revise todos los registros del sistema de punto de venta (POS) y las funciones de procesamiento por lotes para la autorización de crédito, así como cualquier indicio de datos de tarjetahabiente en texto claro.
- ii. Revise todos los reportes de liquidación del POS para asegurarse de que no haya datos de tarjetahabiente sin cifrar.

En caso de que se encuentren datos de tarjetahabiente en texto claro, o de que haya una falla de un control de seguridad del dispositivo o un uso no autorizado comprobado o sospechado de funciones administrativas sensibles, el comercio debe comunicarse de inmediato con el soporte técnico de FreedomPay y seguir las instrucciones de resolución de problemas que se encuentran en la Sección 7 de este documento. Hasta que se

haya restablecido la funcionalidad de cifrado adecuada en el dispositivo y el dispositivo haya sido reautorizado por FreedomPay, el dispositivo defectuoso no podrá utilizarse para procesar transacciones, a menos que el comercio solicite formalmente una suspensión del cifrado P2PE conforme a lo descrito en la Sección 6.2.

5.4 Instrucciones para la resolución de problemas de un dispositivo PTS POI

Si un dispositivo POI está dañado, destruido, parece funcionar mal o de otro modo requiere servicio, el comercio debe seguir el siguiente proceso al interactuar con el personal de FreedomPay:

- i. Comuníquese con el 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 asignado el técnico, FreedomPay proporcionará al comercio los detalles de la solicitud de implementación.
- iv. Cuando el técnico llegue al sitio, y antes de permitirle el acceso al dispositivo POI, el comercio debe verificar la identidad del técnico como empleado o contratista de FreedomPay. Se debe negar el acceso a cualquier otro personal que no valide adecuadamente su identidad.
- v. Una vez verificada la identidad del técnico, el comercio debe asignar a un acompañante para supervisar la actividad del técnico en todo momento.
- vi. Una vez que el técnico haya terminado el trabajo, el comercio debe responder al correo electrónico de despacho con los siguientes detalles:
 - i. Tipo de identificación presentada para la verificación
 - ii. Tiempo que permaneció en la ubicación
 - iii. Número(s) de serie de la(s) terminal(es) que el técnico intervino

Si un comercio ya no desea utilizar los dispositivos POI proporcionados por FreedomPay como parte de un programa de reducción del alcance PCI P2PE debido a una exclusión del comercio, terminación del contrato, cierre del negocio, baja de operaciones u otro motivo, el comercio debe destruir de forma segura todos los dispositivos POI proporcionados por FreedomPay. La destrucción segura debe realizarse mediante el servicio de destrucción segura de FreedomPay, enviando una solicitud a devicedisposal@freedompay.com indicando el número de dispositivos y los números de serie de cada uno. Una vez recibida, el equipo de Professional Services de FreedomPay responderá con más detalles. Para obtener más información sobre posibles servicios de destrucción, comuníquese con su representante de FreedomPay.

6. Transporte / envío de dispositivos PTS POI

6.1 Instrucciones para asegurar que los dispositivos PTS POI se envíen únicamente a sitios/ubicaciones de confianza, según sea necesario (p. ej., para reparación)

Todos los dispositivos enviados al comercio por FreedomPay utilizarán una empresa de mensajería de confianza. A continuación se enumeran algunas de las empresas de mensajería que utiliza FreedomPay, las cuales también podrían ser utilizadas por los comercios para envíos entre ubicaciones:

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

Estas empresas de mensajería se utilizarán para entregar los dispositivos en las direcciones comerciales proporcionadas por el personal del comercio durante la incorporación. En el caso de envíos entre ubicaciones del comercio, los dispositivos solo deben entregarse en direcciones comerciales de confianza. Todos los dispositivos enviados por y hacia el comercio (incluido el envío de una ubicación del comercio a otra) deben empacarse con empaque resistente a la manipulación.

Algunos ejemplos de empaque a prueba de manipulación son sobres o bolsas con etiquetas numeradas que muestran de manera irreversible evidencia de cualquier intento de abrir el paquete. El empaque a prueba de manipulación puede adquirirse con proveedores de artículos de oficina y estará etiquetado específicamente como "Tamper-Proof" o "Tamper-Resistant". Los paquetes también pueden asegurarse con cinta de seguridad contra manipulación alrededor de todas las aberturas.

6.2 Instrucciones para proteger los dispositivos PTS POI destinados al traslado a otras ubicaciones (p. ej., a una instalación de reparación) y durante dicho traslado

Para asegurar la entrega segura de los dispositivos, se recomienda una empresa de mensajería de confianza que permita el rastreo de paquetes y la confirmación de entrega. A continuación se enumeran ejemplos de dichas empresas de mensajería, pero se permiten otros métodos seguros:

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

Todos los dispositivos enviados por y hacia el comercio (incluido el envío de una ubicación del comercio a otra) deben empacarse con empaque resistente a la manipulación.

Algunos ejemplos de empaque a prueba de manipulación son sobres o bolsas con etiquetas numeradas que muestran de manera irreversible evidencia de cualquier intento de abrir el paquete. El empaque a prueba de manipulación puede adquirirse con proveedores de artículos de oficina y estará etiquetado específicamente como "Tamper-Proof" o "Tamper-Resistant". Los paquetes también pueden asegurarse con cinta de seguridad contra manipulación alrededor de todas las aberturas.

7. Orientación / instrucciones adicionales

7.1 Orientación adicional para los comercios sobre la solución P2PE (según sea necesario).

Este Manual de instrucciones de P2PE se proporciona conforme a los requisitos de PCI DSS. La implementación de los controles establecidos en este PIM es un requisito para el SAQ-P2PE de PCI DSS y la Certificación 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 exclusivo riesgo del comercio y puede dar lugar al incumplimiento del SAQ-P2PE de PCI DSS, a la pérdida de la calificación para la reducción del alcance de PCI DSS y/o a la vulneración de la seguridad de los datos.

Al utilizar la solución de reducción del alcance FreedomPay P2PE, el Comercio acepta que no modificará ni intentará modificar ninguna configuración de los dispositivos POI suministrados por FreedomPay, incluidas, entre otras:

- Intentar habilitar cualquier interfaz del dispositivo o mecanismo de captura de datos que haya sido deshabilitado en un dispositivo suministrado por FreedomPay
- Intentar alterar las configuraciones de seguridad o los controles de autenticación
- Abrir físicamente cualquier dispositivo
- Intentar instalar aplicaciones en cualquier dispositivo

Con el fin de mantener la reducción del alcance que ofrece la solución de FreedomPay, el Comercio 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 del alcance P2PE. Las transacciones ingresadas por cualquier otro medio no están sujetas al programa P2PE validado y aprobado por PCI SSC de FreedomPay. FreedomPay ha implementado en su puerta de enlace de pagos (Freeway) un mecanismo para rechazar las transacciones que se envían sin cifrar desde un dispositivo no aprobado por FreedomPay con una respuesta "P2PE Device Error", también conocida como error 266. Estas transacciones sin cifrar no se almacenan en el entorno de FreedomPay, pero pueden almacenarse en los registros generados por el punto de venta del comercio, lo que pone al comercio en riesgo de perder la reducción del alcance de PCI. Si un comercio acepta pagos mediante cualquier otro método fuera de la solución PCI P2PE de FreedomPay o no puede resolver las ocurrencias regulares de errores 266 dentro de los 30 días posteriores a su generación, debe optar por salir del programa de reducción del alcance PCI P2PE mediante el formulario de Solicitud de exclusión del comercio (Apéndice A).

Restricciones por país/región

En caso de que un país o región imponga restricciones sobre qué marca y modelo de dispositivo puede utilizarse 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

Apéndice A: Solicitud de exclusión del comercio

Esta solicitud de exclusión debe ser firmada por un representante autorizado del comercio, según consta en los registros de FreedomPay. Antes de enviar una Solicitud de exclusión del comercio, comuníquese con el Soporte Técnico de FreedomPay para obtener las instrucciones de exclusión. El Soporte Técnico verificará al representante autorizado del comercio y proporcionará un Número de incidente.

Número de incidente (si aplica): _____

Fecha de la solicitud de exclusión: _____

El Comercio que suscribe elige por la presente excluirse de la solución FreedomPay P2PE. Al firmar esta solicitud, el Comercio reconoce que:

1. Las transacciones procesadas mientras la exclusión esté vigente no están sujetas a la reducción del alcance de P2PE.
2. El Comercio es el único responsable de implementar controles alternativos para proteger los datos de cuenta en lugar de la solución FreedomPay P2PE.
3. El Comercio está obligado a informar a su adquirente o a la marca de pago que el Comercio se ha excluido de la solución FreedomPay P2PE.
4. FREEDOMPAY RENUNCIA A TODAS LAS DECLARACIONES Y GARANTÍAS RESPECTO DE LA SOLUCIÓN FREEDOMPAY P2PE EN CUANTO A CADA TRANSACCIÓN PROCESADA MIENTRAS LA EXCLUSIÓN ESTÉ VIGENTE.
5. FREEDOMPAY RENUNCIA A TODA RESPONSABILIDAD, INCLUIDA, ENTRE OTRAS, UNA VULNERACIÓN DE DATOS DERIVADA DE QUE EL COMERCIO PROCESE PAGOS POR MEDIOS DISTINTOS DEL USO DE LA SOLUCIÓN P2PE VALIDADA DE FREEDOMPAY Y DE FREEDOMPAY COMMERCE PLATFORM.
6. El Comercio cuenta con 60 días a partir del 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 FreedomPay y el comercio acuerden mutuamente por escrito una ventana de exclusión diferente. Una vez concluida la ventana de exclusión, es posible que se restrinja al comercio procesar transacciones en FreedomPay Commerce Platform de manera indefinida.

Nota: Tras la exclusión, un comercio puede optar por volver a inscribirse en la solución de reducción del alcance FreedomPay P2PE, sujeto al protocolo de seguridad establecido por FreedomPay, que incluye una certificación del comercio de que todos los remanentes de datos de tarjetahabiente en texto claro se han eliminado de los sistemas del comercio mediante procesos de eliminación segura de datos.

Comercio: _____

Firma: _____

(Nombre del personal autorizado del comercio, en letra de molde)

Nombre: _____

Puesto: _____

(Nombre del personal autorizado del comercio – Firma)

Envíe este formulario por correo electrónico a: compliance@freedompay.com

Apéndice C: Ejemplos de identificación del número de serie de dispositivos POI

Las siguientes imágenes muestran algunos ejemplos de dispositivos POI de diversos fabricantes y la ubicación física de los números de serie aplicados por las instalaciones de inyección de llaves (Key Injection Facilities) para fines de inspección, verificación o RMA de POI (quienes pueden brindar mayor asistencia para ubicar o mapear los números de serie). Para preguntas adicionales sobre los números de serie de los dispositivos POI, comuníquese con compliance@freedompay.com.

Ingenico Lane 3000



Quantum Pay Reader 250



Ziosk

