



Manual de instrucciones de P2PE (PIM)
Guía para comerciantes sobre la
implementación y el mantenimiento de la
solución de reducción del ámbito de
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 del PCI SSC)	
Nombre de la solución P2PE:	FreedomPay Commerce Platform P2PE
Número de referencia del listado de la solución P2PE (Asignado por el 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 de contacto:	Bernard Clary	Cargo:	Vicepresidente de Cumplimiento		
Teléfono:	+1-610-902-9000	Correo electrónico:	compliance@freedompay.com		
Dirección comercial:	FMC Tower at Cira Centre South 2929 Walnut Street · Planta 14	Ciudad:	Philadelphia		
Estado/Provincia:	Pennsylvania	País:	EE. UU.	Código postal:	19104

1.3 Instrucciones de comunicación
Instrucciones sobre cómo ponerse en contacto con el proveedor de la solución P2PE, teniendo en cuenta el establecimiento de un canal/sesión de comunicación de confianza.
<p>Los comerciantes pueden ponerse en contacto con su Customer Success Manager (CSM) dedicado o, accounts@freedompay.com si no tienen un CSM dedicado, para consultas generales relacionadas con su cuenta o implementación.</p> <p>Las consultas de soporte técnico pueden dirigirse a techsupport@freedompay.com o a través del formulario de soporte de nuestra página web.</p> <p>Las consultas de cumplimiento pueden dirigirse a compliance@freedompay.com.</p>

PCI P2PE y PCI DSS

Es posible que se exija a los comerciantes que utilicen esta solución P2PE validar el cumplimiento 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.

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

2. Información sobre los dispositivos PTS POI y el software

2.1 Detalles de los dispositivos 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 del 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 no relacionado con pagos, utilice los números de PIM ID# para consultar las tablas correspondientes a continuación. Los 'PIM ID#' son números creados y utilizados por el proveedor de la solución P2PE únicamente dentro de este PIM para facilitar la referencia cruzada de las aplicaciones P2PE y el software no relacionado con pagos que se utilizan en los dispositivos PTS POI aquí indicados. Los 'PIM ID#' no son asignados por el PCI SSC ni reconocidos por el programa PCI P2PE.

N.º de aprobación PCI PTS	PTS POI Fabricante 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 (PIM ID# de la Tabla 2.2)	Software no relacionado con pagos en dispositivos PTS POI (PIM ID# 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	N/A
4-30257	Ingenico	Lane/8000	LAN80AA, LAN80BA	820547v01.xx	App#1, App#2	N/A

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	N/A
4-30237	Ingenico	Lane/7000	LAN70AA, LAN70AB, LAN70BB	820547v01.xx, 820376v04.xx (Security Services)	App#1, App#2	N/A

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); MOV50DR (CTLS + pantalla de privacidad); MOV50JR (CTLS + pantalla de privacidad + tapa de carcasa de sobremesa); MOV50BE (CTLS); MOV50DE (CTLS + pantalla de privacidad); MOV50JE (CTLS + pantalla de privacidad + tapa de carcasa de sobremesa)</p> <p>MOV50BS (CTLS)</p> <p>MOV50CB (sin CTLS + pantalla de privacidad)</p> <p>MOV50CC (sin CTLS + pantalla de privacidad)</p> <p>MOV50CQ (sin CTLS + pantalla de privacidad)</p> <p>MOV50CS (sin CTLS + pantalla de privacidad)</p> <p>MOV50DB (CTLS + pantalla de privacidad)</p> <p>MOV50DC (CTLS + pantalla de privacidad)</p> <p>MOV50DN (CTLS + pantalla de privacidad)</p> <p>MOV50DQ (CTLS + pantalla de privacidad)</p> <p>MOV50DS (CTLS + pantalla de privacidad)</p> <p>MOV50JB (CTLS + pantalla de privacidad + tapa de carcasa de sobremesa)</p>	<p>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)</p>	App#1, App#2, App#3, App#5	N/A
---------	----------	---------------------------	--	--	--	---------------------

			<p>MOV50JC (CTLS + pantalla de privacidad + tapa de carcasa de sobremesa)</p> <p>MOV50JN (CTLS + pantalla de privacidad + tapa de carcasa de sobremesa)</p> <p>MOV50JQ (CTLS + pantalla de privacidad + tapa de carcasa de sobremesa)</p> <p>MOV50JS (CTLS + pantalla de privacidad + tapa de carcasa de sobremesa)</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 (base firmware)</p>	<i>App#1, App#2, App#3</i>	<i>N/A</i>
4-20317	Ingenico	<i>DESK/5000</i>	<p>(CTLS) (sin CTLS + pantalla de privacidad) (sin CTLS) DES50AB, DES50BB, DES50CB, DES50DB (CTLS + pantalla de privacidad)</p>	<p>820376v01.xx, 820547v01.xx (Core Firmware), 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>N/A</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>	N/A	N/A

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		N/A
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	N/A	N/A
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 (Core Firmware, 820376v12.xx (Security Services), 820555v01.xx (SRED AWL), 820556V01.xx (SRED On-Guard SDE), 820549V01.xx (SRED On-Guard FPE), 820570V07.xx (Open Protocols), 820565V01.xx (SRED FF1)	App#2	<i>N/A</i>
4-30381	Ingenico	<i>Self/2000</i>	SEL20AA	820376v04.xx (Servicios de seguridad) 820566v01.xx	App#2	<i>N/A</i>
4-30393	Ingenico	<i>Self/4000</i>	SEL40BA	820376v04.xx (Servicios de seguridad) 820547v01.xx	App#2	<i>N/A</i>
4-30384	Ingenico	<i>Self/5000</i>	SEL50CA	820376v04.xx (Servicios de seguridad) 820566v01.xx	App#2	<i>N/A</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>N/A</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>N/A</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>N/A</i>

4-20359	Ingenico	Move/5000	MOV50BE (CTLS) MOV50BQ (CTLS) MOV50BR (CTLS) MOV50BS (CTLS) MOV50DC (CTLS + pantalla de privacidad) MOV50DE (CTLS + pantalla de privacidad) MOV50DN (CTLS + pantalla de privacidad) MOV50DQ (CTLS + pantalla de privacidad) MOV50DR (CTLS + pantalla de privacidad) MOV50DS (CTLS + pantalla de privacidad) MOV50JC (CTLS + tapa de carcasa de sobremesa) MOV50JE (CTLS + tapa de carcasa de sobremesa) MOV50JN (CTLS + pantalla de privacidad + tapa de carcasa de sobremesa) MOV50JQ (CTLS + tapa de carcasa de sobremesa) MOV50JR (CTLS + tapa de carcasa de sobremesa) MOV50JS (CTLS + tapa de carcasa de sobremesa) 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	N/A
---------	----------	---------------------------	---	--	---	---------------------

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 (Open Protocols), 820572V01.xx (Tetra JVM Addon), 820376v14.xx (Servicios de seguridad)	App#2	N/A
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 (Open Protocols), 820376v14.xx (Servicios de seguridad)	App#2	N/A
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	N/A

4-30533	Ingenico	Link/2500 LE	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)	App#2	N/A
4-30498	Ingenico	AXIUM RX7000	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)	App#4	SW#1
4-30444	Ingenico	AXIUM EX8000	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)	App#4	SW#1
4-30443	Ingenico	AXIUM DX8000-2, AXIUM DX8000-5	D851x3 (with 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)	App#4	SW#1
4-30527	Ingenico	AXIUM RX5000	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)	App#4	SW#1
4-90075	ID Tech	SREDKey 2	80172001 (con MSR), 80172002 (sin MSR), 80172004 (con MSR), 80172005 (sin MSR)	SREDKEY2 FW v1.00.xxx.xxx.S, SREDKey2 FW v1.01.xxx.xxx.S	N/A	N/A

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	N/A	
4-30432	Infinite Peripherals, Inc	QuantumPay Reader 250	06.00.xx.xx	3.0.xx.xx	N/A	N/A
4-30433	Infinite Peripherals, Inc	QuantumPay Reader 300	05.11.xx.xx	3.1.xx.xx, 3.2.xx.xx	N/A	N/A
4-30437	Infinite Peripherals, Inc	QuantumPay PIN 400	00xxxD1xxxxxx (versión sin CTLS) CLxxxD1xxxxxx (versión CTLS)	3.1.xx.xx, 3.2.xx.xx	N/A	N/A
4-30438	Infinite Peripherals, Inc	QuantumPay Connected 150	PRR05xxx PRR15xxx PXR05xxx PXR15xxx	3.0.xx.xx, 3.1.xx.xx	N/A	N/A
4-30511	Infinite Peripherals, Inc	QuantumPay Connected 250 and 252	51DxxxxNxxxx versión sin CTLS 51DxxxxCxxxx versión CTLS	3.0.xx.xx	N/A	N/A
4-30453	Infinite Peripherals, Inc	QuantumPay PIN 401	41D1xxxN0xxx 41D1xxxC0xxx	3.0.xx.xx	N/A	N/A
4-30464	Infinite Peripheral, Inc	QuantumPay PIN 451	41D1xxxN1xxx - versión sin CTLS 41D1xxxC1xxx - versión CTLS	3.0.xx.xx	N/A	N/A

4-30318	Datecs 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	N/A	N/A
---------	-------------	--	--	------------------------	-----	-----

4-30475	Infinite Peripherals, Inc	<i>QuantumPay Pro Plus</i>	21.1x.xx.xxx	SP: 3.0.xx.xx, AP: 1.0.xx.xx	N/A	N/A
4-80037	Castles Technology Co. Ltd	<i>Saturn 1000-E</i>	SATURN1000E-HW- V1.20.xxxx	1.1.1.xxxxxx	N/A	<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	N/A	<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	N/A	<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:	N/A	<i>SW#1-22</i>
4-80094	Castles Technology Co. Ltd	<i>S1F4 PRO</i>	HW-V-1G.00	1.6.1.xxxxxx	N/A	<i>SW#1-22</i>
4-80082	Castles Technology Co. Ltd	<i>S1P</i>	HW-V1.00	1.4.1.xxxxxx	N/A	<i>SW#1-22</i>
4-80092	Castles Technology Co. Ltd	<i>S1P2</i>	HW-V-1D.00	1.6.1.xxxxxx	N/A	<i>SW#1-22</i>
4-80091	Castles Technology Co. Ltd	<i>S1Mini2</i>	HW-V-1E.00	1.6.1.xxxxxx	N/A	<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	N/A	<i>SW#1-22</i>
4-80106	Castles Technology Co. Ltd	<i>S1U2-M4</i>	HW-V-1I.00	1.6.1.xxxxxx	N/A	<i>SW#1-22</i>

4-80084	Castles Technology Co. Ltd	S2L	HW-V1A.00	1.4.1.xxxxxx	N/A	SW#1-22
4-80077	Castles Technology Co. Ltd	S1U2	HW-V1.00	1.4.1.xxxxxx 1.4.2.xxxxxx	N/A	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.xxx+ap 5.xxx.xxx.xxx+p 6.xxx.xxx.xxx+ap 6.xxx.xxx.xxx+p	N/A	N/A
4-90136	Ziosk	Z600	6.0.A 6.0.B	6201.29.xxxx.xxx.xxx 6201.30.xx.x.xxx	N/A	N/A
4-90335	Ziosk	Z600 Pro	6.0.A	6201.29.xxxx.xxx.xxx	N/A	N/A
4-30522	Verifone	M425 M450	H625-0007-0090-1xx-xxx-B0 (con pantalla de privacidad), H650-0007-0090-0xx-xxx-B0 (sin pantalla de privacidad), H650-0007-0090-1xx-xxx-B0 (con pantalla de privacidad), H625-0007-0090-0xx-xxx-B0 (sin pantalla 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	N/A	N/A
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	N/A	N/A

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	N/A	<i>N/A</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	N/A	<i>N/A</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	N/A	<i>N/A</i>
4-40363	PAX Computer Technology (Shenzhen) Co Ltd	<i>A6650</i>	A6650-0xx-0x6-0xxx (SIN CTLS), A6650-0xx-0x6-1xxx (SIN CTLS), A6650-0xx-Rx6-0xxx (CTLS), A6650-0xx-Rx6-1xxx (CTLS),	26.00.01 xxxxx	N/A	<i>N/A</i>
4-30554	Toast Inc	<i>TG300, TG310</i>	REV1.xx	01.xx.xx.-10xxxxx	N/A	<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 en esta solución P2PE. Por definición, las aplicaciones P2PE tienen acceso a datos de cuenta en texto claro. Estas aplicaciones **deben** indicarse en el listado de la solución P2PE.

Los 'PIM ID#' son números creados y utilizados por el proveedor de la solución P2PE únicamente dentro de este PIM para 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 el PCI SSC ni reconocidos por el programa PCI P2PE.

Nota: Las aplicaciones P2PE que se han evaluado como parte de la solución P2PE y para las que se decidió no incluirlas en un listado independiente 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

PIM ID# (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 aplicación PCI P2PE (Asignado por el 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	FreeWay Standalone Application (FSA)	3.0.x	2025-00909.015

2.3 Detalles del software no relacionado con pagos

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

*Por definición, el software P2PE no relacionado con pagos **no debe** tener acceso alguno a datos de cuenta en texto claro. Aunque este tipo de software se evalúa como parte de la evaluación de la solución P2PE, no figura en el listado de soluciones PCI P2PE.*

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

PIM ID# (p. ej., SW#1, SW#2, ...)	Proveedor del software no relacionado con pagos	Nombre del software no relacionado con pagos	Versión(es) del software no relacionado con pagos	Información adicional (según sea necesario)
SW#1	FreedomPay	CX App	1.x.x	Componente middleware de Android para la integración 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 no relacionado con pagos

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 gestión de inventario, la resolución de problemas y la notificación de incidentes.

Instrucciones para confirmar el hardware y el firmware del dispositivo PTS POI, así como las aplicaciones P2PE y el software no relacionado con pagos presentes

Las versiones de hardware se encuentran 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 front-end
2. Encienda el dispositivo mediante el cable de alimentación o conectándolo a un PC con el cable USB
3. Durante el arranque del dispositivo, pulse la siguiente secuencia de teclas en el dispositivo Ingenico: 2634, [botón verde], F
4. Si su dispositivo no tiene 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. Anote la información de firmware asociada a M1

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

Dispositivos ID Tech:

Las versiones de firmware de estos dispositivos solo pueden verse mediante una aplicación proporcionada por ID Tech. Para descargar esta aplicación, póngase en contacto con compliance@freedompay.com para obtener ayuda.

Dispositivos Castles/Elo:

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

Dispositivos Ziosk:

La versión del firmware puede verse en el menú del dispositivo, en Settings > About device > Firmware version.

Dispositivos Infinite Peripheral:

Las versiones de firmware de estos dispositivos solo pueden verse mediante una aplicación proporcionada por Infinite Peripherals. Para descargar esta aplicación, póngase en contacto con compliance@freedompay.com para obtener ayuda.

Dispositivos PAX

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

Dispositivos Toast

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

Dispositivos Verifone

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

2.5 Inventario y supervisión de los dispositivos PTS POI

- Todos los dispositivos PTS POI deben documentarse mediante procedimientos de control de inventario y supervisión, incluido el estado del dispositivo (p. ej., implementado, pendiente de implementación, en reparación o fuera de uso por otro motivo, o en tránsito).
- Este inventario debe realizarse, como mínimo, con periodicidad anual.
- Cualquier discrepancia en el inventario, incluidos los dispositivos PTS POI extraviados o sustituidos, debe notificarse a el proveedor de la solución P2PE a través de la información de contacto y las instrucciones de la Sección 1 anterior.
- La siguiente tabla de inventario de muestra es solo ilustrativa. El comerciante debe registrar y mantener el inventario real en un documento externo.

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

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

- Implementado
- Pendiente 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 comerciantes 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 comerciante también debe establecer un “sistema estatal de contabilidad y control” para llevar el seguimiento de todos los dispositivos POI (cantidad y tipo), anotar los cambios en los inventarios de materiales (entrantes/salientes) y supervisar todos los aspectos del ciclo de vida del dispositivo POI mientras esté en posesión y bajo el control del comerciante. Registre todas las discrepancias de inventario en su sistema de control de inventario y notifique a FreedomPay los dispositivos extraviados o perdidos, una vez identificados, en compliance@freedompay.com, o al socio/revendedor designado de FreedomPay que suministró los dispositivos.

Si su organización es multitienda, regional o un operador nacional, es importante emplear sistemas de gestión y seguimiento de inventario a nivel local, regional y nacional para garantizar que el conocimiento y la capacidad para gestionar, rastrear y notificar 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 siguiente. Toda la información de identificación específica del dispositivo necesaria para el seguimiento del inventario puede encontrarse en una etiqueta en el panel posterior o en el compartimento de la batería de cada dispositivo POI (en el **Apéndice C de la Sección 9, Orientación adicional, se incluyen imágenes de la ubicación del número de serie de una muestra de dispositivos** y/o a través de la interfaz lógica del dispositivo POI.)

El comerciante debe desarrollar y mantener protocolos escritos para la reubicación de dispositivos entre sus locales. El comerciante debe supervisar 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 más información sobre el mantenimiento de la cadena de custodia en la reubicación o el almacenamiento de dispositivos, póngase en contacto con compliance@freedompay.com o con el socio/revendedor de FreedomPay que suministró los dispositivos.

Es posible que se solicite al comerciante que presente su inventario anual de POI a su adquirente como parte de su cumplimiento anual de PCI DSS. El incumplimiento de los controles indicados en el PIM puede dar lugar a la “exclusión del comerciante”, es decir, la suspensión del programa de reducción del alcance P2PE de FreedomPay Commerce Platform.

Si un comerciante deja de querer utilizar los dispositivos POI proporcionados por FreedomPay como parte de un programa de reducción del alcance PCI P2PE debido a la exclusión del comerciante, la rescisión del contrato, el cierre del negocio, la retirada de servicio u otro motivo, el comerciante 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 dispositivo. Una vez recibida, el equipo de Professional Services de FreedomPay responderá con más detalles. Para obtener más información sobre posibles servicios de destrucción, póngase en contacto con su representante de FreedomPay.

Tabla de inventario de muestra

Fabricante 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 garantizar que los dispositivos PTS POI proceden de fuentes/sitios/ubicaciones de confianza

FreedomPay o su KIF certificado enviará al comerciante un correo electrónico de notificación previa al envío en el que se identificarán los números de serie de los dispositivos POI, el nombre del transportista, el número de seguimiento, las instalaciones desde las que se envió el paquete y la ubicación de comerciante aprobada a la que se envió el paquete.

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

- i. Inspeccionar el embalaje según lo indicado anteriormente.
- ii. Verificar que el transportista identificado en el albarán de entrega sea un transportista de confianza.
- iii. Verificar que el paquete se envió desde unas instalaciones de proveedor asociadas con uno o más proveedores de componentes incluidos en FreedomPay's Commerce Platform P2PE, o desde unas instalaciones que formen parte de la cadena de custodia preestablecida del comerciante. Si no está seguro de la dirección o ubicación desde la que debería proceder un dispositivo, póngase en contacto con compliance@freedompay.com.
- iv. Verificar que los números de serie del albarán 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 de estado y ubicación del dispositivo.

El comerciante debe devolver inmediatamente 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 un transportista de confianza o que haya sido enviado desde una ubicación distinta de unas instalaciones esperadas.

Antes de devolver un dispositivo POI a unas instalaciones de proveedor aprobadas, el comerciante debe enviar un correo electrónico a poidevicereturns@freedompay.com para determinar adónde debe enviarse el dispositivo según la situación.

3.2 Instrucciones para confirmar que el dispositivo PTS POI y su embalaje no han sido manipulados

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

- Verificar el transportista identificado en el albarán de entrega
- Verificar que el paquete se envió desde unas instalaciones esperadas.
- Verificar que los números de serie del albarán de envío coincidan con los números de serie del correo electrónico de notificación previa al envío.
- Verificar que el embalaje no esté dañado hasta el punto de dejar expuesto el interior del paquete.
- Verificar que el embalaje no se haya mojado hasta el punto de que la humedad haya penetrado en las paredes del embalaje.
- Verificar que la integridad del embalaje con evidencia de manipulación esté intacta.

Ejemplo de un paquete no manipulado con cinta con evidencia de manipulación:



Si el dispositivo o el embalaje no superan alguna de las inspecciones anteriores, póngase en contacto con su representante de FreedomPay y devuelva el dispositivo según 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 concederle acceso a los dispositivos PTS POI.

En la mayoría de los casos, FreedomPay podrá prestar soporte de dispositivos de forma remota sin necesidad de asistencia in situ. Sin embargo, durante instalaciones complejas o en determinados casos de soporte, puede enviarse un técnico a la ubicación de un comerciante. Si se necesita un técnico de FreedomPay in situ, asegúrese de seguir los siguientes pasos antes, durante y después de que se realice el trabajo in situ.

- i. Se asignará un técnico de campo al caso y este completará una solicitud de envío.
- ii. Una vez asignado un técnico, FreedomPay proporcionará al comerciante los detalles de la solicitud.
- iii. Cuando el técnico llegue a las instalaciones y antes de permitirle el acceso al dispositivo POI, el comerciante debe verificar la identidad del técnico como empleado o contratista de FreedomPay. Debe denegarse el acceso a cualquier otro personal sin la validación adecuada de su identidad.
- iv. Una vez verificada la identidad del técnico, el comerciante debe asignar a un acompañante para supervisar 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. Tipo de documento de identidad presentado para la verificación
- ii. Tiempo transcurrido en la ubicación
- iii. (Solo para casos de soporte) Número(s) de serie del/de los terminal(es) manipulado(s) por el técnico

FreedomPay nunca enviará técnicos in situ sin coordinarse previamente con los contactos del comerciante y proporcionar información sobre el técnico enviado a efectos de verificación. No debe concederse 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 estén en su poder, incluidos los dispositivos:

- Pendientes de implementación
- En reparación o fuera de uso por otro motivo
- 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 indicarse en el listado de la solución P2PE.

Si se utiliza algún dispositivo que no figure en la Tabla 2.1 para aceptar datos de cuentas de pago, podría verse afectada la elegibilidad del comerciante para utilizar el SAQ P2PE; póngase en contacto 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 comerciante para utilizar el SAQ P2PE; póngase en contacto con su adquirente o con las marcas de pago.

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

- Habilitar interfaces del dispositivo o mecanismos de captura de datos que estén deshabilitados
- 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 cada instalación de dispositivo POI mediante uno de los siguientes métodos o una alternativa aprobada por su Evaluador de Seguridad Cualificado (QSA):

- i. El dispositivo está montado físicamente o sujeto con cable para evitar su retirada, manipulación o sustitución no autorizadas. Los métodos aceptables incluyen:
 - a. Montar el dispositivo en un soporte de seguridad para PIN aprobado
 - b. Asegurar el dispositivo mediante un candado con cable acoplado a la ranura de seguridad del dispositivo POI y fijado de forma permanente al mostrador o a otro elemento físico seguro en el extremo opuesto del cable. Existe una amplia variedad de candados con cable disponibles en la mayoría de las tiendas de informática, en línea o a través de FreedomPay. Póngase en contacto con su representante de FreedomPay si necesita ayuda para encontrar un candado con cable adecuado.
- ii. El dispositivo debe ubicarse de forma que el personal autorizado pueda observarlo/supervisararlo fácilmente y en un entorno que disuada los intentos de vulneración.

Los pasos de implementación adicionales incluyen:

- 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 de la parte inferior del dispositivo.
 - i. Para obtener ayuda para localizar los números de serie de los dispositivos POI, consulte la sección del **Apéndice C en la Sección 9, Orientación adicional**.
 - b. Actualizar el sistema de registro de dispositivos para reflejar el cambio de estado y 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. Móvil (celular)

Otro: para los tipos de comunicación de POI no indicados anteriormente, el comerciante debe ponerse en contacto con compliance@freedompay.com para obtener 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 atestación oficial de FreedomPay que indique que el tipo de comunicación de POI, no incluido 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 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 retirada o manipulación no autorizadas. El dispositivo debe ubicarse de forma que el personal autorizado pueda observarlo/supervisarlos 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 a 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 retirada y/o sustitución no autorizadas

Se anima a los comerciantes a montar los dispositivos en servicio en un soporte de seguridad para PIN aprobado o a asegurarlos mediante un candado con cable acoplado a la ranura de seguridad del dispositivo POI y fijado de forma permanente en el extremo opuesto del cable. Existe una amplia variedad de candados con cable disponibles en la mayoría de las tiendas de informática o en línea.

Póngase en contacto con su representante de FreedomPay o con su QSA si necesita ayuda para encontrar un candado con cable adecuado. Para implementaciones no propicias para dispositivos montados (p. ej., dispositivos independientes o situaciones móviles), deben aplicarse procedimientos para mitigar el riesgo de manipulación o vulneración del dispositivo. Esto puede incluir la asignación del dispositivo al personal del local, 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 se reciban dispositivos POI de FreedomPay antes de su instalación, cuando se traspasen desde otras ubicaciones de comerciante aprobadas 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 acceder y existen mecanismos/políticas para documentar todo acceso físico al área de “almacenamiento seguro”, incluidos:

- 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 de la persona, empresa, motivo del acceso y horas 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 es y dónde se encuentra el área de almacenamiento seguro, así como los procedimientos establecidos para cumplir los requisitos establecidos en esta sección.

5. Supervisión e inspección continuas de los dispositivos PTS POI implementados

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

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

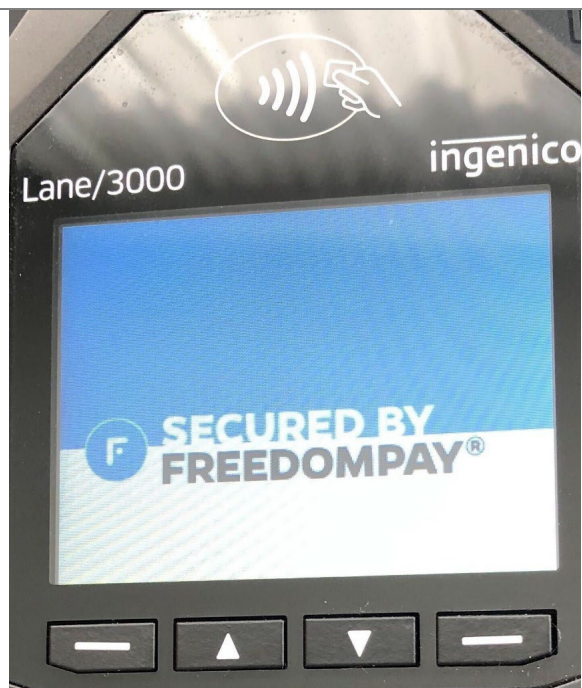
- ¿Se ha dañado o alterado de alguna manera el cable USB/Ethernet?
- ¿Coincide el número de serie del dispositivo con el número de serie proporcionado por FreedomPay? (Consulte el Apéndice C para ver la ubicación del número de serie)
- ¿Están los dispositivos POI activos protegidos adecuadamente según el PIM?
- ¿Están los dispositivos POI inactivos almacenados de forma segura según el PIM?
- ¿Se ha dañado el dispositivo POI 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 precintos de seguridad, etiquetas o marcas ocultas?

Ejemplos de áreas de inspección:

Verifique que no se hayan retirado los tornillos exteriores.



Verifique que la pantalla “Secured by FreedomPay” esté presente.



Si un comerciante implementa un dispositivo POI de FreedomPay en un área que no esté supervisada físicamente por un empleado aprobado del comerciante, deben existir procedimientos adecuados para reducir la posibilidad de manipulación del dispositivo y, en el peor de los casos, el tiempo transcurrido entre la vulneración y su detección. Consulte a su Evaluador de Seguridad Cualificado (QSA) independiente para obtener más información sobre la inspección y supervisión de POI.

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

El comerciante debe devolver inmediatamente 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 un transportista de confianza o que haya sido enviado desde una ubicación distinta de unas instalaciones de proveedor aprobadas.

Envío de dispositivos POI:

- i. Los dispositivos POI solo pueden ser transportados por un transportista de confianza a unas instalaciones de proveedor aprobadas indicadas 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 , que generará una etiqueta de envío para la devolución.
- iii. Todos los números de serie de los dispositivos POI deben estar impresos en el albarán de embalaje o en la etiqueta de envío.

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

5.2 Instrucciones para inspeccionar los dispositivos PTS POI en busca de dispositivos de skimming y responder ante una sospecha de detección de skimming

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

Compruebe si hay superposiciones o herramientas insertadas en los puntos de interacción.



Compruebe si hay cables/conexiones o hardware adicionales en el punto de conexión.



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

En caso de un fallo de cifrado indicado por la presencia de un código de error 266 o un mensaje “P2PE Encryption Error”, se recomienda que el comerciante:

- 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 titulares de tarjetas en texto claro.
- ii. Revise todos los informes de liquidación del POS para asegurarse de que no haya datos de titulares de tarjetas sin cifrar.

Si se encuentran datos de titulares de tarjetas en texto claro, o si se produce un fallo de un control de seguridad del dispositivo o un uso no autorizado, comprobado o sospechado, de funciones administrativas sensibles, el comerciante debe ponerse en contacto inmediatamente con el soporte técnico de FreedomPay y seguir las instrucciones de resolución de problemas que figuran en la Sección 7 de este documento. Hasta que se

haya restablecido la funcionalidad de cifrado adecuada en el dispositivo y este haya sido reautorizado por FreedomPay, el dispositivo defectuoso no podrá utilizarse para procesar transacciones, salvo que el comerciante solicite formalmente una suspensión del cifrado P2PE según se describe 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 requiere de otro modo mantenimiento, el comerciante debe seguir el siguiente proceso al interactuar con el personal de FreedomPay:

- i. Póngase en contacto con el soporte técnico de FreedomPay en el 888-495-2446 o por correo electrónico en techsupport@freedompay.com.
- ii. Si el técnico de soporte de FreedomPay determina que debe enviarse un técnico de campo, este completará una solicitud de envío.
- iii. Una vez asignado un técnico, FreedomPay proporcionará al comerciante los detalles de la solicitud de implementación.
- iv. Cuando el técnico llegue a las instalaciones y antes de permitirle el acceso al dispositivo POI, el comerciante debe verificar la identidad del técnico como empleado o contratista de FreedomPay. Debe denegarse el acceso a cualquier otro personal sin la validación adecuada de su identidad.
- v. Una vez verificada la identidad del técnico, el comerciante debe asignar a un acompañante para supervisar 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 envío con los siguientes detalles:
 - i. Tipo de documento de identidad presentado para la verificación
 - ii. Tiempo transcurrido en la ubicación
 - iii. Número(s) de serie del/de los terminal(es) manipulado(s) por el técnico

Si un comerciante deja de querer utilizar los dispositivos POI proporcionados por FreedomPay como parte de un programa de reducción del alcance PCI P2PE debido a la exclusión del comerciante, la rescisión del contrato, el cierre del negocio, la retirada de servicio u otro motivo, el comerciante 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 dispositivo. Una vez recibida, el equipo de Professional Services de FreedomPay responderá con más detalles. Para obtener más información sobre posibles servicios de destrucción, póngase en contacto con su representante de FreedomPay.

6. Transporte/envío de dispositivos PTS POI

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

Todos los dispositivos enviados al comerciante por FreedomPay utilizarán un transportista de confianza. A continuación se enumeran algunos de los transportistas utilizados por FreedomPay, que también podrían ser utilizados por los comerciantes para envíos entre ubicaciones:

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

Estos transportistas se utilizarán para entregar los dispositivos en 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 entregarse en direcciones comerciales de confianza. Todos los dispositivos enviados por y al comerciante (incluidos los envíos entre ubicaciones del comerciante) deben embalarse con embalaje resistente a la manipulación.

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

6.2 Instrucciones para proteger los dispositivos PTS POI destinados a ser transportados a otras ubicaciones (p. ej., a un centro de reparación) y durante dicho transporte

Para garantizar la entrega segura de los dispositivos, se recomienda un transportista de confianza que permita el seguimiento de paquetes y la confirmación de entrega. A continuación se enumeran ejemplos de dichos transportistas, aunque se permiten otros métodos seguros:

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

Todos los dispositivos enviados por y al comerciante (incluidos los envíos entre ubicaciones del comerciante) deben embalarse con embalaje resistente a la manipulación.

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

7. Orientación / instrucciones adicionales

7.1 Orientación adicional para los comerciantes 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 del SAQ-P2PE de PCI DSS y de la Atestación de Cumplimiento. El uso de cualquier dispositivo POI no aprobado por FreedomPay y/o cualquier incumplimiento de los requisitos establecidos en este manual corre por cuenta y riesgo exclusivos del comerciante 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 P2PE de FreedomPay, el comerciante acepta que no modificará ni intentará modificar ninguna configuración de los dispositivos POI suministrados por FreedomPay, incluido, entre otros:

- Intentar habilitar interfaces del dispositivo o mecanismos de captura de datos que hayan sido deshabilitados en un dispositivo suministrado por Freedom Pay
- Intentar alterar las configuraciones de seguridad o los controles de autenticación
- Abrir físicamente cualquier dispositivo
- Intentar instalar aplicaciones en cualquier dispositivo

Para mantener la reducción del alcance que ofrece la solución de FreedomPay, el comerciante reconoce que todas las transacciones con tarjeta de crédito deben introducirse/deslizarse a través de un dispositivo POI aprobado para permanecer en el programa de reducción del alcance P2PE. Las transacciones introducidas por cualquier otro medio no están sujetas al programa P2PE validado de FreedomPay aprobado por el PCI SSC. FreedomPay ha implementado en su pasarela de pago (Freeway) un mecanismo para rechazar las transacciones enviadas 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 comerciante, lo que pone al comerciante en riesgo de perder la reducción del alcance de PCI. Si un comerciante acepta pagos por cualquier otro método ajeno a la solución PCI P2PE de FreedomPay o no puede resolver las apariciones periódicas de errores 266 en un plazo de 30 días desde su generación, debe darse de baja del programa de reducción del alcance PCI P2PE mediante 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 la marca y el modelo de dispositivo que pueden utilizarse dentro de sus fronteras, se actualizará la siguiente tabla:

País/Región	Marca del dispositivo	Modelo del dispositivo
-------------	-----------------------	------------------------

Australia	Ingenico	Lane 5000, Move 5000
Australia	IDTech	SREDKey v2

Apéndice A: Solicitud de exclusión del comerciante

Esta solicitud de exclusión debe estar firmada por un representante autorizado del comerciante, tal y como figure en los registros de FreedomPay. Antes de presentar una solicitud de exclusión del comerciante, póngase en contacto con el soporte técnico de FreedomPay para obtener las instrucciones de exclusión. El soporte técnico verificará al representante autorizado del comerciante y proporcionará un número de incidente.

Número de incidente (si procede): _____

Fecha de la solicitud de exclusión: _____

El comerciante abajo firmante opta por excluirse de la solución P2PE de FreedomPay. Al firmar esta solicitud, el comerciante reconoce que:

1. Las transacciones procesadas mientras la exclusión esté en vigor no están sujetas a la reducción del alcance de P2PE.
2. El comerciante es el único responsable de implementar controles alternativos para proteger los datos de cuenta en lugar de la solución P2PE de FreedomPay.
3. El comerciante está obligado a informar a su adquirente o marca de pago de que se ha excluido de la solución P2PE de FreedomPay.
4. FREEDOMPAY RECHAZA TODAS LAS DECLARACIONES Y GARANTÍAS RELATIVAS A LA SOLUCIÓN P2PE DE FREEDOMPAY EN CUANTO A CADA TRANSACCIÓN PROCESADA MIENTRAS LA EXCLUSIÓN ESTÉ EN VIGOR.
5. FREEDOMPAY RECHAZA TODA RESPONSABILIDAD, INCLUIDA, ENTRE OTRAS, UNA VULNERACIÓN DE DATOS DERIVADA DE QUE EL COMERCIANTE PROCESA PAGOS SIN UTILIZAR LA SOLUCIÓN P2PE VALIDADA DE FREEDOMPAY Y FREEDOMPAY COMMERCE PLATFORM.
6. El comerciante dispone de 60 días desde el momento de la exclusión ("periodo de exclusión") para resolver las condiciones que motivaron la exclusión y volver a inscribirse en la solución, salvo que FreedomPay y el comerciante acuerden mutuamente por escrito un periodo de exclusión diferente. Tras el periodo de exclusión, se podrá restringir al comerciante el procesamiento de transacciones en FreedomPay Commerce Platform de forma indefinida.

Nota: Tras la exclusión, un comerciante puede optar por volver a inscribirse en la solución de reducción del alcance P2PE de FreedomPay, sujeto al protocolo de seguridad establecido por FreedomPay, incluida una atestación del comerciante de que todos los restos de datos de titulares de tarjetas en texto claro se han eliminado de los sistemas del comerciante mediante procesos seguros de eliminación de datos.

Comerciante: _____

Firma: _____

(Nombre del personal autorizado del comerciante - en letra de imprenta)

Nombre: _____

Cargo: _____

(Nombre del personal autorizado del comerciante – 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 varios fabricantes y la ubicación física de los números de serie aplicados por las instalaciones de inyección de claves a efectos de inspección, verificación o RMA de POI (quienes pueden ayudar con la ubicación o el mapeo de los números de serie). Para más preguntas sobre los números de serie de los dispositivos POI, póngase en contacto con compliance@freedompay.com.

Ingenico Lane 3000



Quantum Pay Reader 250



Ziosk

