REPÚBLICA DOMINICANA
JUNTA CENTRAL ELECTORAL
COMITE DE COMPRAS Y CONTRATACIONES

JUNTA CENTRAL ELECTORAL
Comité de Compras y Contrataciones

CCC-JCE-480-2025

Santo Domingo, D.N.,
30 de diciembre, 2025.

A los : Interesados en el Concurso por Comparación de Precios Ref.: JCE-CCC-CP-2025-0032, destinado a la adquisición de lectores RFID.

Asunto : Respuestas.

Actuando en nombre y representación del Comité de Compras y Contrataciones, en atención a las respuestas, aclaraciones y enmiendas, tenemos a bien responder lo siguiente:

1) **A fin de asegurar una correcta interpretación de las especificaciones técnicas**, agradeceríamos confirmar si la institución acepta que los requisitos de seguridad, captura de PIN y lectura de documentos electrónicos puedan ser cubiertos mediante una arquitectura integrada de estación de enrolamiento, compuesta por más de un dispositivo especializado, siempre que, en conjunto, se cumpla con la totalidad de los requerimientos establecidos.

   Respuesta: *No. La Ficha Técnica requiere un* ***dispositivo unificado****. Se especifica la adquisición de "Terminales de Entrada de PIN Seguros" que deben integrar internamente tanto el "Módulo Lector RFID/NFC" (capacidad Contactless), exigido en los requerimientos funcionales (FT3), como el "módulo de seguridad de hardware interno dedicado" para la gestión de claves. De igual forma, se exige en el FT2 que el dispositivo posea la capacidad intrínseca de cifrar el PIN en origen antes de salir del mismo, lo cual requiere una integración de hardware en una sola unidad para garantizar que la clave de cifrado nunca sea expuesta al Host. Esto descarta una arquitectura de múltiples dispositivos separados para estas funciones.*

2) **Considerando que los estándares PCI PTS y los protocolos ICAO Doc 9303** corresponden a dominios tecnológicos distintos, agradeceríamos confirmar si la institución prevé la aceptación de soluciones integradas que cumplan cada estándar en su respectivo componente certificado, manteniendo una operación unificada dentro de la estación de enrolamiento.

   Respuesta: *El dispositivo debe cumplir con ambos estándares* ***simultáneamente en la misma unidad física****. El requerimiento* ***SN1*** *exige certificación PCI PTS Versión 5.x ó superior para la seguridad física y lógica del dispositivo, mientras que los requerimientos* ***FT3*** *y* ***SN3*** *(Estándares de Identidad Digital) exigen que el dispositivo integre un módulo lector que asegure "Compatibilidad con la arquitectura de seguridad y los protocolos de acceso a datos del chip (ej. PA, AA, BAC, EAC, SAC, PACE) definidos en las normativas* ***ICAO (Doc 9303)****" dentro del mismo.*

3) ¿Podría la institución confirmar si se considerarán aceptables soluciones que cumplan los requisitos mediante **equivalencia funcional**, aun cuando dichos requerimientos se encuentren distribuidos en componentes certificados e integrados, siempre que el resultado operativo, de seguridad y normativo sea equivalente o superior al solicitado?

Respuesta: *No. La Ficha Técnica define requisitos de hardware específicos que implican una unidad integrada, no distribuida. Por ejemplo, el requisito FT10 establece que "El dispositivo debe poseer un módulo de seguridad de hardware interno dedicado" para el aislamiento criptográfico. Permitir componentes distribuidos violaría el requisito de cifrado en origen (FT2) y aislamiento criptográfico dentro del dispositivo de captura (SN1, FT10).*

4) **Para efectos de claridad técnica y correcta preparación de las ofertas**, ¿podría la institución precisar si los requisitos técnicos deben ser cumplidos por un único dispositivo físico, o si es aceptable que se satisfagan mediante una solución integrada por varios dispositivos, debidamente certificados e interoperando de forma segura?

Respuesta: *Sí, deben ser cumplidos por un único dispositivo físico. Las especificaciones describen un "dispositivo" (singular) que integra teclado físico (FT1), lector NFC (FT3) y módulo de seguridad (FT10). Además, la sección de conectividad (FT6) especifica interfaces USB para la integración del dispositivo con el Host, lo cual implica una unidad periférica única que concentre todas las funciones.*

5) **Considerando que el uso declarado no corresponde a una transacción financiera**, ¿es obligatorio que el equipo completo esté listado como PCI PTS aprobado en el sitio oficial del PCI SSC, o basta con que el módulo de captura de PIN cumpla con dicha certificación?

Respuesta: ***Sí, es obligatorio.*** *El requisito **SN1** establece explícitamente: "El dispositivo debe estar listado como aprobado en la web oficial de PCI SSC". La justificación técnica aclarada en el pliego es que, aunque no se trate de una transacción financiera, este es el estándar global más estricto para proteger la captura de PIN contra ataques físicos y lógicos (skimming, tampering).*

6) ¿El teclado puede ser integrado digital en el equipo y la llave de seguridad?

Respuesta: ***No.*** *El requisito **FT1** (Teclado de PIN seguro) exige un "Teclado físico robusto, ergonómico, retroiluminado y resistente al vandalismo". Se especifica, además, que debe contar con "teclas numéricas estándar y teclas de funciones" (mínimo 15 teclas físicas), descartando la opción de teclados digitales o en pantalla (touch).*

NOTA: Les recordamos que el plazo para preguntas venció en fecha 23/12/2025.

Atentamente,

JUNTA CENTRAL ELECTORAL
Comité de Compras y Contrataciones

ANA YSABEL SALVADOR M.
Coordinadora

AYSM/np/vd.-