

## **Consultas Realizadas**

# **Licitación 480955 - ADQUISICIÓN DE CERTIFICADOS Y DISPOSITIVOS CUALIFICADOS - FIRMA DIGITAL**

## Consulta 1 - Licitación ID 480955 - ADQUISICIÓN DE CERTIFICADOS Y DISPOSITIVOS CUALIFICADOS - FIRMA DIGITAL.

Consulta	Fecha de Consulta	28-04-2026
<p>Nos dirigimos a la Convocante con relación a las Especificaciones Técnicas detalladas en la Sección V del PBC, específicamente en los ítems 1 y 2, donde se solicita la provisión de "certificado de firma digital + dispositivo (token)". Considerando que el sistema de adjudicación es por el "Total", solicitamos respetuosamente a la Convocante evaluar la modificación de las especificaciones técnicas para estandarizar el requerimiento hacia la tecnología de firma digital remota (Formato F3), eliminando la dependencia de dispositivos físicos (tokens - Formato F2). Fundamentamos esta solicitud en los siguientes beneficios operativos y de seguridad para la Circunscripción Judicial:</p> <ul style="list-style-type: none"> <li>- Mayor Seguridad y Respaldo: En el formato F3, la clave privada se encuentra resguardada en un dispositivo de alta seguridad criptográfica (HSM) administrado por un Prestador de Servicios de Certificación (PCSC). En contraste, el formato F2 depende de un dispositivo físico (USB/Token) susceptible a extravíos, robos o daños físicos, comprometiendo potencialmente la clave y requiriendo reposiciones físicas (las cuales están previstas en la garantía de los bienes del pliego).</li> <li>- Movilidad y Accesibilidad: El formato F3 permite a los Magistrados, Actuarios y Jefaturas firmar desde cualquier computadora que tenga el software firmador instalado, eliminando la barrera de portar un dispositivo físico en todo momento. El formato F2 exige un proceso estrictamente manual y presencial frente al equipo (Usuario + Token físico + PC).</li> <li>- Integración Tecnológica (Expediente Electrónico): Siendo el destino principal el marco del Expediente Electrónico, el formato F3 permite una integración nativa y transparente con sistemas institucionales (APIs, SDKs, plataformas), optimizando los flujos de trabajo de la institución.</li> <li>- Gestión Centralizada: Al ser el F3 gestionado por el PCSC, se reduce significativamente la carga administrativa y de soporte técnico local para la Sección Informática, en comparación con la logística de entrega, configuración y mantenimiento de tokens físicos.</li> </ul> <p>¿Sería factible que la Convocante emita una Adenda modificando las especificaciones para que todos los ítems soliciten certificados bajo la modalidad F3 (HSM/Nube), optimizando así los recursos del Estado y garantizando una mejor experiencia para el usuario final?</p>		

Respuesta	Fecha de Respuesta	29-04-2026
<p>Si bien reconocemos los avances tecnológicos asociados al modelo F3, consideramos que la modalidad F2 continúa ofreciendo ventajas sustanciales en términos de seguridad, control, operatividad e independencia tecnológica, las cuales detallamos a continuación, en contraposición a los beneficios expuestos:</p> <ul style="list-style-type: none"> <li>- Seguridad y Control de la Clave Privada: En el formato F2, la clave privada se encuentra almacenada en un dispositivo criptográfico físico (token) bajo control exclusivo del usuario titular, lo que garantiza un modelo de seguridad basado en posesión física + autenticación personal. A diferencia del modelo F3, donde la clave reside en infraestructura de terceros (HSM en la nube), el F2 elimina la dependencia de entornos externos, reduciendo la superficie de ataque asociada a accesos remotos, vulnerabilidades en servicios cloud o posibles brechas en prestadores de certificación. Además, el token requiere interacción física directa, lo que mitiga riesgos de uso indebido, accesos remotos no autorizados o ataques automatizados. Asimismo, la logística de tokens, si bien implica gestión física, también otorga mayor trazabilidad y control individualizado sobre los dispositivos y su uso.</li> <li>- Independencia Tecnológica y Disponibilidad: El modelo F3 introduce una dependencia directa de disponibilidad de servidores del PCSC Integridad de APIs o plataformas externas esto puede representar un riesgo operativo en escenarios críticos, en cambio con el modelo F2 dependemos exclusivamente de nuestras plataformas + el token físico donde la firma puede realizarse sin interrupciones. Por las razones expuestas, mantenemos la especificación técnica actual del PBC.</li> </ul>		