**LISTA DE REQUISITOS A CONSULTAR POR CONSORCIO**

En el marco del proceso de evaluación técnica y como parte de la verificación de las propuestas recibidas, a continuación, se presenta el listado de requisitos para los cuales **se requiere que los oferentes proporcionen las aclaraciones y/o explicaciones técnicas que, para cada requisito, permitan verificar, validar y comprender que se satisfacen de conformidad con lo ofertado.**

|  |
| --- |
| **CONSORCIO EMDOC** |
| **2.1** | **Especificaciones de máquina de impresión** |
| 2.1.13 | La máquina debe tener su propio PC integrado con su propio sistema operativo y software de la máquina. |
| 2.1.14 | El sistema operativo de la PC debe ser WINDOWS. Las impresoras pueden ser WINDOWS o LINUX. |
| 2.1.22 | La calidad de las impresoras debe mantenerse a lo largo de los diez años de la contratación. Tendrán garantía mínima por dos (2) años. Cada oferente, debe indicar en su propuesta, la vida útil de las piezas de cada impresora que produce el láser y queda comprometido a que su solución de impresión mantendrá la calidad de las impresoras durante todo el tiempo que lo exige el contrato, obligándose a reemplazar lo necesario y las veces que sea conveniente para cumplir con esta exigencia de calidad de las impresoras. |
| 2.1.24 | El proveedor deberá incluir 230 lectores de chip sin contacto, y poner como opcional, la compra de lectores de forma individual. La caracteristicas del lector de tarjetas debe ser Lector para NFC Compatible con ISO 14443 Tipo A, Tipo B y Tarjetas Mifare 1k&4k, ICAO 9303 con interoperabilidad OACI DOC 9303, ISO18013, PA, AA, BAC, EAC , SAC. |
| **2.2** | **Personalización** |
| 2.2.21 | Los sistemas de personalización deben estar equipados con el software interno de gestión de datos, que proporciona interfaces de usuario claras e iguales para la integración en la red del proyecto. El equipo deberá preparar los datos para realizar la personalización de las credenciales de forma totalmente automática. |
| **3.1** | **Características generales de la PKI** |
| 3.1.5 | El proveedor deberá proporcionar un portal para firma de documentos con el estándar ISO 32000-1, además de la integración a las aplicaciones de la JCE que permita firmar con certificados tanto en la cédula de identidad o externos .El portal para Firmar documentos debe manejar al menos tres tipos de roles: 1. Administrador, con todos los permisos, esta figura debe poder generar y/o enrolar Agentes Certificadores; 2. Agente Certificador con permisos para enrolar y/o generar certificados para los usuarios finales o firmantes; 3. Firmante, son los usuarios que podrán firmar los documentos. |
| 3.1.10 | El oferente deberá incluir en su propuesta, toda la infraestructura física necesaria para la implantación, ejecución y mantenimiento de la PKI, el conjunto de hardware y software en las instalaciones que indique la dirección de informática. El contrato de mantenimiento a cotizar será de dos (2) años. A partir de los dos años, la JCE podrá renovar el mantenimiento con el precio establecido del proveedor de forma anual. Para la solución de la PKI el ambiente productivo debe habilitarse en alta disponibilidad con 2 nodos activos en balanceo de carga, un ambiente de DRP en disponibilidad simple (1 nodo) y un ambiente de desarrollo en disponibilidad simple (1 nodo). |
| 3.1.12 | En la Nube (compatible con los servicios en la nube de Azure): CMS, CRL/Protocolo de Estado del Certificado en Línea, Repositorio PKI, y servicios adicionales no críticos |
| 3.1.13 | Tanto la PKI de firma de documentos como la PKI de Firma Digital deben cumplir CC EAL 4+ |
| **3.2** | **Autoridad de Certificación (CA) de firma de país (CSCA)** |
| 3.2.3 | Los sistemas o instalaciones propuestos deberán estar bien protegidos de cualquier acceso externo o no autorizado a través del diseño inherente y las instalaciones de seguridad de hardware y requerirá medidas de seguridad robustas, entre otras: - Autenticación multifactorial (MFA para acceso a la administración). Cifrado avanzado en todas las comunicaciones y datos almacenados, utilizando algoritmos criptográficos robustos y actuales.- Uso de Módulos de Seguridad por Hardware (HSMs) certificados (FIPS 140-2 nivel 2 o superior) para la generación y almacenamiento de claves privadas.- Implementación de sistemas avanzados de monitoreo y detección de intrusos (IDS/IPS).- El monitoreo debe incluir de infraestructura, de seguridad y de comunicaciones- Segmentación de redes que aísle la infraestructura de PKI de otras redes corporativas.- Mantenimiento de todos los sistemas y software de la PKI actualizados con los últimos parches de seguridad.- Realización de auditorías regulares y evaluaciones de seguridad.- Capacitación del personal involucrado en la operación y gestión de la PKI sobre las mejores prácticas de seguridad y procedimientos de respuesta a incidentes. |
| **3.2.11** | **Algoritmos criptográficos asimétricos (podrá soportar)** |
| 3.2.11.1 - 3.2.11.9 | [ RSA, DSA, ECC, ECDSA, ECDH, Ed25519, ECIES, Brainpool curves (nombrados y definidos por el usuario), Diffie Hellman (DH) ] |
| **3.2.12** | **Algoritmos criptográficos simétricos (podrá soportar)** |
| 3.2.12.1 - 3.2.12.10 | [ AES, AES-GCM, DES, 3DES, ARIA, SEED, RC2, RC4, RC5, CAST ] |
| **4** | **Especificaciones de la tarjeta de identidad digital** |
| 4.2 | Estar preparada para cumplir con el estándar de la OACI (“Guiding Core Principles for the Development of Digital Travel Credential (DTC) de octubre de 2020” |
| 4.5 | Los datos entregados deberán ser firmados electrónicamente. Esta firma electrónica certificada de los datos permitirá que terceros puedan validar la integridad y procedencia de los datos que presenta el ciudadano. Los datos entregados deberán ser firmados electrónicamente por la JCE. Esta firma electrónica certificada de los datos permitirá que terceros puedan validar la integridad y procedencia de los datos que presenta el ciudadano, tanto la firma de los datos como la validación de estos, se realizará usando los certificados electrónicos administrados por la JCE, como Autoridad Certificadora descrita en el apartado Infraestructura de clave pública. |
| **4.7** | **Aspectos generales de la tarjeta digital** |
| 4.7.36 | Capacidad de Servicio: Atender al menos 5,000 solicitudes diarias de credenciales digitales. La solución debe ser Modular y escalable para adaptarse a la evolución en la demanda de este tipo de documentos. El oferente deberá́ proporcionar información de dimensionamiento de la plataforma. |