ANEXO
CERTIFICADO DE HOMOLOGACIÓN

a) CÓDIGO: ATT-DJ-RA-H-TL LP 39/2020

b) EMISIÓN Y VENCIMIENTO: 28 de enero del 2020, vence el 27 de enero del 2025

c) CONDICIONES DE OTORGACIÓN DE LA HOMOLOGACIÓN: Reconocimiento y verificación de una certificación internacional

d) CATEGORÍA Y SUBCATEGORÍA DENTRO DE LAS CUALES EL EQUIPO FUE HOMOLOGADO

CATEGORIA	Software de aplicación o aplicativo de la Infraestructura Nacional de Certificado Digital
SUBCATEGORIA	Software de aplicación para la generación de par de claves

e) NOMBRE Y DIRECCIÓN DEL DESARROLLADOR:

AGENCIA PARA EL DESARROLLO DE LA SOCIDAD
DE LA INFORMACIÓN EN BOLIVIA – ADSIB
Calle Jaime Mendoza No 981, Zona San Miguel
La Paz – Bolivia

f) DATOS TÉCNICOS:

Aplicación	CERTIFICADO POR SOFTWARE - ADSIB
Desarrollador	ADSIB
Versión	1.0

g) ESPECIFICACIONES TÉCNICAS PRINCIPALES:

ESPECIFICACIONES TÉCNICAS PRINCIPALES	
Sistema Operativo	Debian 9 "Stretch"
Compatibilidad de Sistemas Operativos	Linux (Debian 9,10 y Ubuntu 18) Windows (Ver. 7 y 10)
Lenguaje para el Desarrollo	C++
Tipo de Autenticación y Control de Acceso	Cifrado simétrico por contraseña mediante algoritmo AES CBC con aplicación a clave privada y el certificado
Soporte API del cliente y Estándares	PKCS#12
Algoritmos Criptográficos	AES CBC RSAES-PKCS1-v1_5
Algoritmo de Hash	SHA-256
Longitud de Clave RSA	2048

I-LP-1652

Nivel de Seguridad FIPS140-2	Nivel 1
Tipo de Generación de Números Aleatorios	Pseudo-Aleatorios (PRNG)
Certificación Internacional	Certificado NIST #1747 https://csrc.nist.gov/projects/cryptographicmodule-validation-program/Certificate/1747
Sobre el Software	
Versiones (Revisión)	URL: https://gitlab.softwarelibre.gob.bo/adsib/certificado-software Versión 1.0
Programa Fuente (Última Versión)	URL: https://gitlab.softwarelibre.gob.bo/adsib/certificadosoftware/-/archive/master/certificado-software-master.tar.gz. Publicada y liberada
Código o Programa Ejecutable	URL: https://firmadigital.bo/software
Versión Final de Software de Aplicación MS5 o SHA1	
https://gitlab.softwarelibre.gob.bo/adsib/certificado-software/-/archive/final/certificadosoftware-final.tar.gz	843cf3fa2ce62f149546f6ef0acfb80239707f0d
https://gitlab.softwarelibre.gob.bo/adsib/certificado-software/-/archive/final/certificadosoftware-final.zip	9ce33f237a821d4915f7e3392d961fd5ca411285

h) AUDITORIA INFORMATICA:

ORGANISMO AUDITOR	AGETIC
REPORTE O INFORME DE LA AUDITORIA INFORMATICA	AGETIC-UCGII/IT/0323/2019 AGETIC-UCGII/IT/0344/2019

Nota.-
i) El desarrollador del software de aplicación o aplicativo para la generación de claves, es responsable de la correcta generación del par de calves para los propósitos del servicio de Certificación Digital.
ii) Toda entidad Certificadora, debe hacer uso de un software de aplicación o aplicativo registrado en la ATT.

D.T.S.T. - T.I.C. V°B° A.E.R. A.T.T.

DIRECCIÓN JUR. V°B° L.A.K.K.

I-LP-1652