ANEXO

FECHA DE EMISION:	12 de Octubre del 2021	CÓDIGO:	ATT-DJ-RA-H-TL LP 638/2021
FECHA DE VENCIMIENTO:	11 de Octubre del 2026		

CERTIFICADO DE HOMOLOGACIÓN

1	CATEGORÍA (S)	Software de aplicación o aplicativo de la Infraestructura Nacional de Certificado Digital
2	SUBCATEGORIA (S)	Software de aplicación para la generación de par de claves
3	NOMBRE Y DIRECCIÓN DEL FABRICANTE	AGENCIA PARA EL DESARROLLO DE LA SOCIDAD DE LA INFORMACIÓN EN BOLIVIA – ADSIB Calle Jaime Mendoza No 981, Zona San Miguel La Paz – Bolivia

	APLICACIÓN	DESARROLADOR	VERSIÓN
4	Jacobitus Total	ADSIB	1.0.2

5	ORGANISMO AUDITOR	AGETIC	REPORTE O INFORME DE LA AUDITORIA INFORMATICA
			AGETIC-CGII/IT/0049/2021 AGETIC-CGII/IT/0053/2021

	TECNOLOGÍA	*Software de Aplicación para la Generación de Par de Claves*
6	SISTEMA OPERATIVO	Debian 10 "Buster"
7	COMPATIBILIDAD DE SISTEMAS OPERATIVOS	Windows, Linux y MacOS
8	LENGUAJE PARA EL DESARROLLO	Java
9	TIPO DE AUTENTICACIÓN Y CONTROL DE ACCESO	Cifrado simetrico por contrasena mediante el algoritmo pbeWithSHAAnd3-KeyTripleDESCBC aplicado a la clave privada y el certificado.
10	SOPORTE API DEL CLIENTE Y ESTÁNDARES	PKCS#12
11	ALGORITMOS CRIPTOGRÁFICOS	pbeWithSHAAnd3-KeyTripleDES-CBC RSAES-PKCS1-v1_5
12	ALGORITMO DE HASH	SHA-256

E-D-4577

Resolución Administrativa Homologación

13	**LONGITUD DE CLAVE RSA**	2048
14	**NIVEL DE SEGURIDAD FIPS140-2**	Nivel 1
15	**TIPO DE GENERACIÓN DE NÚMEROS ALEATORIOS**	Pseudo-Aleatorios (PRNG)
16	**CRIPTOGRAFÍA BASE**	BouncyCastle
	Sobre el Software	
17	**VERSIONES (REVISIONES)**	URL: https://gitlab.softwarelibre.gob.bo/adsib/jacobitus4
18	**PROGRAMA FUENTE (ÚLTIMA VERSIÓN)**	URL: https://gitlab.softwarelibre.gob.bo/adsib/jacobitus4/-/tree/final
19	**CÓDIGO O PROGRAMA EJECUTABLE**	URL: https://firmadigital.bo/jacobitus4/
	Versión Final de Software de Aplicación MS5 o SHA1	
20	https://gitlab.softwarelibre.gob.bo/adsib/jacobitus4/-/archive/final/jacobitus4-final.tar.gz	9019d77d5d2f04b689e7f74e6a565f3f4349cc79
21	**CONDICIÓN DE LA HOMOLOGACIÓN**	Reconocimiento y verificación mediante un Organismo Auditor

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.

iii) El Informe Técnico Jurídico es parte integrante de la Resolución Administrativa como documento que respalda la información en el presente Certificado.

V°B° H.M.D. A.T.T.

V°B° A.T.T.

ANALISTA LEGAL V°B° L.F.F.L. A.T.T.

E-D-4577