POLÍTICAS DE SEGURIDAD

DAVISIGN V.2.0



Lima, febrero de 2023

INDICE

1. PREAMBULO ……1

2. TRATAMIENTO DE LOS DATOS ……..1

3. AUTENTICIDAD DEL SOFTWARE ……..2

4. AUTENTICIDAD DEL MODULO ……2

1. PREÁMBULO

Dado el incesante desarrollo y avance de las tecnologías de la información, a través del cual la información como principal activo viaja a un ritmo vertiginoso y constante por medio del Internet y, consciente de la importancia de los datos personales y del peligro que puede generar su tratamiento de modo indiscriminado, es necesario asegurar la protección de los datos personales sin crear barreras innecesarias que limiten los flujos de información, asimismo, es necesario garantizar la confidencialidad de los datos personales de carácter privado y de la información confidencial.

En ese sentido, el Software o módulo de firma digital DAVISIGN, reconoce la importancia de implementar medidas de seguridad orientadas a asegurar el adecuado tratamiento de los datos personales recolectados como parte del ejercicio de sus acciones, así como garantizar la confidencialidad de la información y la protección de los datos personales de carácter privado de sus Usuarios[1].

La presente Política abarca la manera en que los datos o información personal son recolectados, utilizados, tratados y transferidos. Asimismo, es objeto del presente documento establecer las directrices que todo el usuario del presente documento deberá de cumplir, a fin de asegurar el adecuado tratamiento de los datos personales y la confidencialidad de la información, evitando así posibles incidencias de seguridad como: pérdida, tratamiento o acceso no autorizado, fuga o robo de información, entre otros.

2. TRATAMIENTO DE LOS DATOS

Para todos los efectos de la prestación de servicios de firma digital por medio del módulo DAVISIGN garantiza que ningún dato o información es almacenada del documento origen (documento a firmar digitalmente).

El usuario programador o integrador de software debe garantizar que ninguna se eliminen correctamente los archivos originados a partir de este módulo siendo su responsabilidad el buen uso o destino de los documentos producidos.

3. AUTENTICIDAD DEL SOFTWARE

[1] Para efecto del presente documento entiéndase como Usuario a los titulares y/o suscriptores de certificados digitales, en concordancia con lo dispuesto por el Artículo 9º del Reglamento de la Ley de Firmas y Certificados Digitales.

El modulo denominado DAVISIGN se encuentra firmado por lo cual su integridad puede ser comprobada en cualquier momento, esto para evitar falsificación o suplantación y mal uso en un proceso de firma digital.

EL usuario programador que haga referencia a este módulo debe garantizar que el canal establecido entre su software y el módulo de firma digital es seguro y que no es espiado por algún tipo de software malicioso. Esta responsabilidad recae sobre el programador o especialista en integración.

4. AUTENTICIDAD DEL MODULO

No está permitido alterar o desensamblar el código del módulo de firma digital DAVISIGN, de ser hecho esta acción es responsabilidad del usuario y/o programador alertar y bloquear su uso.

DAVISIGN únicamente brinda respaldo sobre los documentos firmados digitalmente por este y bajo las condiciones establecidas en este documento.