POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

Certificaciones Digitales Digicert S.R.L.

0. GESTIÓN DEL DOCUMENTO

	Elaborado por	Revisado por	Aprobado por
Nombre	Miguel Gutiérrez	Fabio Cortez	Bernardo Chumacero
Cargo	Oficial de Seguridad	Responsable de Desarrollo	Representante Legal
Fecha	2026-09-07	2026-09-07	2026-09-07
Firma	Firmado digitalmente por Miguel Angel Gutierrez Blanco 08/09/2026 12:57 A	Firmado digitalmente por Fabio Cortez Medrano	Firmado digitalmente por Bernardo Fabian Chumacero Ruiz 08/09/2026 17:11

1. CONTROL DE CAMBIOS

1.1. Cambios a la política

Esta política será revisada al menos una vez al año, con el objetivo de incorporar los cambios derivados de los avances tecnológicos, así como las modificaciones en la estructura organizativa de la empresa, en las regulaciones y en las normas externas aplicables.

1.2. Detalle de cambios

Revisión	Fecha	Detalle de modificaciones
0	2023-12-04	Versión inicial del documento.
1	2026-09-07	Complementación del documento en atención a las observaciones formuladas por la ATT. Se incorporan las secciones de Flujo Operativo, Consentimiento del Titular y Medidas de Seguridad para el Resguardo de los Datos Sensibles, y se precisa el plazo de conservación de los datos personales.

2. OBJETO

La Entidad Certificadora considera relevante la implementación de una regulación integral sobre la protección de los datos personales que cursan a través de las Tecnologías de la Información y Comunicación (TIC), con el propósito de otorgar seguridad y resguardar la intimidad del usuario que navega en la red.

https://www.viafirma.com.do/inbox/app/digicert/v/49dff218-18eb-4ba7-b963-17e3752db9b5

3. INTRODUCCIÓN

Descripción del servicio

El certificado digital emitido por Digicert S.R.L. permite al cliente realizar firmas digitales avanzadas y autenticar su identidad con validez legal, vinculándolo jurídicamente con el documento digital o mensaje electrónico de datos y garantizando la integridad de este. La certificación que emite Digicert S.R.L. comprende tanto a personas naturales como a personas jurídicas.

La firma digital consiste en un par de claves criptográficas, una pública y otra privada, aplicadas mediante una función matemática a los documentos digitales. La clave privada permanece siempre en posesión del firmante y es la utilizada para generar las firmas; la clave pública se divulga y es la utilizada para verificar la firma de otro sujeto.

Todo lo descrito se encuentra respaldado por la Resolución Administrativa Regulatoria ATT-DJ-RAR-TL LP 202/2019, emitida por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT), por la Ley N° 164, Ley General de Telecomunicaciones y Tecnologías de Información y Comunicación, y por su Decreto Supremo reglamentario N° 1793.

4. CONCEPTOS FUNDAMENTALES

Para efectos de la presente política, se adoptan las siguientes definiciones:

a) Archivo o banco de datos: designan indistintamente al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento físico, electrónico, magnético o informático, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.

b) Autorización: consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales por una Entidad Certificadora Autorizada.

c) Cesión de datos: toda revelación de datos realizada a una persona distinta del titular de los datos.

d) Consentimiento del titular: toda manifestación de voluntad libre, inequívoca, específica e informada, mediante la cual el titular consiente el tratamiento de los datos personales que le conciernen.

e) Datos personales: toda información de cualquier tipo referida a personas individuales o colectivas determinadas o determinables.

f) Datos sensibles: datos personales que revelen filiación política o filosófica, credo religioso, ideología o afiliación sindical, así como las informaciones referentes a origen racial y étnico, salud u orientación sexual.

g) Destinatario: persona individual o colectiva, pública o privada, que reciba una cesión de datos, se trate o no de un tercero.

h) Disociación de datos: todo tratamiento de datos personales realizado de manera tal que la información obtenida no pueda vincularse a persona determinada o determinable.

i) Encargado del tratamiento: persona individual o colectiva, pública o privada, que sola o en conjunto con otros trate datos personales por cuenta del responsable del archivo o banco de datos o del tratamiento.

j) Tercero: persona individual o colectiva, pública o privada, distinta del titular del dato, del responsable del archivo o banco de datos o del tratamiento, del encargado y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable o del encargado del tratamiento.

k) Responsable del tratamiento: persona individual o colectiva, pública o privada, propietaria del archivo o banco de datos, o que decida sobre la finalidad, el contenido y el uso del tratamiento.

l) Titular de los datos: persona natural o jurídica a quien se refiere la información que reposa en un archivo o banco de datos.

m) Tratamiento de datos personales: cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, el almacenamiento, el uso, la circulación o la supresión.

n) Usuario de datos: toda persona, pública o privada, que realice a su arbitrio el tratamiento de datos, ya sea en un archivo o banco de datos propio o a través de conexión con los mismos.

o) Fuentes accesibles al público: aquellos archivos o bancos de datos cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación.

p) Firma digital: conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permite verificar su integridad, así como identificar de forma unívoca y vincular jurídicamente al autor con el documento.

q) Protección de datos personales: resguardo de toda información concerniente a una persona natural o jurídica que la identifica o la hace identificable.

r) Servicio de certificación digital: consiste en emitir, revocar y administrar los certificados digitales utilizados para generar firmas digitales.

s) Servicio de registro: consiste en comprobar y validar la identidad del solicitante de un certificado.

5. PRINCIPIOS

Los servicios de certificación digital, en cuanto al tratamiento de datos personales, se rigen por los siguientes principios:

https://www.viafirma.com.do/inbox/app/digicert/v/49dff218-18eb-4ba7-b963-17e3752db9b5

Principio de finalidad.

La utilización y el tratamiento de los datos personales por parte de las entidades certificadoras autorizadas deben obedecer a un propósito legítimo, el cual debe ser de conocimiento previo del titular.

Principio de veracidad.

La información sujeta a tratamiento debe ser veraz, completa, precisa, actualizada, verificable e inteligible, quedando prohibido el tratamiento de datos incompletos o que induzcan a error.

Principio de transparencia.

Se garantiza el derecho del titular a obtener de la entidad certificadora autorizada, en cualquier momento y sin impedimento alguno, información relacionada con la existencia de los datos que le conciernen.

Principio de seguridad.

Se implementan los controles técnicos y administrativos que se requieran para preservar la confidencialidad, integridad, disponibilidad, autenticidad, no repudio y confiabilidad de la información, brindando seguridad a los registros y evitando su falsificación, extravío, utilización y acceso no autorizado o fraudulento.

Principio de confidencialidad.

Todas las personas que intervienen en el tratamiento de datos personales están obligadas a garantizar la reserva de la información, incluso después de finalizado su vínculo con alguna de las actividades que comprende el tratamiento, pudiendo únicamente realizar el suministro o la comunicación de datos personales cuando ello corresponda al desarrollo de las tareas autorizadas.

6. DERECHOS DE LOS TITULARES DE DATOS

Los titulares de los datos tienen los siguientes derechos:

a) Derecho de información y contenido de la información.

b) Derecho a conocer los datos registrados.

c) Derecho de rectificación, actualización, inclusión o eliminación.

d) Datos sensibles. Ninguna persona puede ser obligada a proporcionar datos sensibles, tales como ideología, religión, salud u origen racial o étnico, entre otros. Estos solo podrán ser objeto de tratamiento con el consentimiento expreso y escrito del titular y/o cuando medien razones de interés.

https://www.viafirma.com.do/inbox/app/digicert/v/49dff218-18eb-4ba7-b963-17e3752db9b5

7. FLUJO OPERATIVO

La recopilación de la información de los titulares se realiza a través de las plataformas Agencia de Registro, Plataforma Web Servicios En Línea y RA Digicert, en las cuales el signatario gestiona la solicitud para la adquisición de su certificado digital. Dicha recopilación se efectúa conforme al siguiente flujo:

a) El titular se registra en la plataforma Servicios En Línea para solicitar su certificado.

b) Se captura la información personal del titular y se valida contra el ente gubernamental competente (SEGIP).

c) Se captura la información biométrica del titular correspondiente a su documento de identidad (anverso y reverso), a efectos de validar su identidad.

d) Se captura la selfie biométrica del titular.

e) Se registra la solicitud del titular en la plataforma RA Digicert.

f) Se notifica al titular el contrato de adhesión correspondiente.

8. CONSENTIMIENTO DEL TITULAR

a) El titular manifiesta su consentimiento en las plataformas mediante la marcación de una casilla de verificación, desde la cual accede al texto de la presente Política de Protección de Datos Personales.

b) El consentimiento otorgado es almacenado y puede ser consultado en la sección de auditoría de las plataformas.

c) Junto con el consentimiento se resguarda la fecha y hora en que se realizó la operación.

d) El registro del consentimiento se conserva de manera permanente en la plataforma.

9. INFORMACIÓN QUE ES RECOPILADA

La información que es recopilada desde la plataforma web está en función al tipo de persona que requiere los servicios, es decir, si se trata de una persona natural o de una persona jurídica. En cada caso se solicita la siguiente información:

a) Personas naturales

Ciudad de ingreso de la solicitud
Nombres del titular
Apellido paterno del titular
Apellido materno del titular

Fecha de nacimiento del titular
Número de celular del titular
Correo electrónico
Tipo de documento
Número de documento de identidad
Complemento (si corresponde)
Expedición del documento de identidad
Dirección del domicilio
Adjunto: copia del anverso del documento de identidad
Adjunto: copia del reverso del documento de identidad
Adjunto: aviso de cobranza de servicio público (agua o luz)

b) Personas jurídicas

Ciudad de ingreso de la solicitud
Nombres del titular
Apellido paterno del titular
Apellido materno del titular
Fecha de nacimiento del titular
Número de celular del titular
Correo electrónico
Tipo de documento
Número de documento de identidad
Complemento (si corresponde)
Expedición del documento de identidad
Número de Identificación Tributaria
Nombre de la organización
Unidad organizacional (opcional)
Cargo en la organización
Dirección del domicilio (representante legal)
Dirección de ubicación de la organización
Adjunto: copia del anverso del documento de identidad (titular)
Adjunto: copia del reverso del documento de identidad (titular)
Adjunto: carta de autorización
Adjunto: copia del Número de Identificación Tributaria
Adjunto: copia del anverso del documento de identidad (representante legal)
Adjunto: copia del reverso del documento de identidad (representante legal)
Adjunto: poder del representante legal

https://www.viafirma.com.do/inbox/app/digicert/v/49dff218-18eb-4ba7-b963-17e3752db9b5

10. CÓMO USAMOS LA INFORMACIÓN PROVISTA POR EL TITULAR DE LOS DATOS

Los datos personales registrados y la información adjunta descritos en el punto anterior se utilizan para las siguientes finalidades:

a) Realizar las validaciones y contrastaciones de datos con el SEGIP, a fin de garantizar la veracidad de los datos ingresados.

b) Generar los contratos entre el titular y Certificaciones Digitales Digicert.

c) Procesar la generación y emisión del certificado digital.

d) Procesar la generación de firmas de los documentos adjuntados por el titular.

e) Emitir la correspondiente facturación por el uso del servicio.

f) Permitir que los operadores internos revisen, observen o aprueben toda la información enviada.

g) Contactar al titular de los datos en el momento en que se lo requiera.

h) Enviar la información procesada referente a contratos generados, formularios, certificado emitido y documentos firmados.

11. MEDIDAS DE SEGURIDAD PARA EL RESGUARDO DE LOS DATOS SENSIBLES

a) Como primera medida de seguridad, el acceso a las plataformas se realiza mediante registros de usuario, a los cuales se asigna el privilegio de información que corresponde a la función que desempeñan.

b) La información se encuentra resguardada en los servidores de Digicert, con control de acceso restringido y limitado únicamente al personal autorizado.

c) Se realizan respaldos diarios de la información.

d) Como medida de protección, cada funcionario suscribe un documento de confidencialidad que lo obliga a resguardar toda información técnica, comercial, financiera y de cualquier otra naturaleza a la que tenga acceso.

12. MODIFICACIÓN O ACTUALIZACIÓN DE LOS DATOS REGISTRADOS

La modificación o actualización de los datos registrados es procesada conforme a los dos siguientes escenarios:

a) Cuando está en proceso de emisión del certificado. Mientras el certificado no haya sido emitido ni se haya generado el contrato, es posible realizar correcciones o actualizaciones de los datos ingresados.

b) Cuando el certificado ya fue emitido. Una vez emitido el certificado, solamente podrá actualizarse el correo electrónico para el reenvío de alguna información requerida por el titular, previo envío de la carta de solicitud.

13. CONSERVACIÓN DE LOS DATOS PROVISTOS POR EL TITULAR DE LOS DATOS

La Entidad Certificadora retiene los datos personales y la información recopilada a través de los formularios de registro de la plataforma web con fines operativos, de registro, de validación y legales. Dichos datos personales se conservan por un periodo de diez (10) años, computados desde el vencimiento o la revocación del certificado, a efectos de cumplir con las finalidades descritas en la presente política.

https://www.viafirma.com.do/inbox/app/digicert/v/49dff218-18eb-4ba7-b963-17e3752db9b5