



REGISTRO PÚBLICO DE PANAMÁ
DIRECCIÓN NACIONAL DE FIRMA ELECTRÓNICA
CERTIFICADOS ELECTRÓNICOS CALIFICADOS DE
AUTENTICACIÓN DE SITIOS WEB



Licencia de uso y aceptación de condiciones

_____, ____ de _____ de _____

Sr./Sra. _____

con número de cédula de identidad / pasaporte _____

fecha de nacimiento _____

y dirección de correo electrónico _____

declara haber recibido los Certificados Electrónicos Calificados de autenticación de sitios Web, para autenticación y firma electrónica calificada solicitados, confirmando la exactitud de su contenido y comprometiéndose a utilizarlos de acuerdo con lo dispuesto en: 1-la presente licencia de uso, 2-la Política de Certificación de Certificados de Autenticación de Sitios Web y 3-la Declaración de Prácticas de Certificación (DPC) para la infraestructura de clave pública del Registro Público de Panamá (RPP-PKI) y las cuales pueden consultarse en la página web <http://www.pki.gob.pa/normativa/index.html>. Asimismo, declara que conoce que el uso de las claves privadas certificadas es personal e intransferible y está limitado a los usos especificados en la Política de Certificación de Certificados de Autenticación de Sitios Web establecidos por el Registro Público de Panamá, por lo que el solicitante asume la responsabilidad por el mal uso, como de los perjuicios que de éste pudieran derivarse.

Sr./Sra. _____

certifica que, en su presencia y en su condición de operador de la Autoridad de Registro de la Infraestructura de Clave Pública del Registro Público de Panamá ha generado en un dispositivo adecuado a tal efecto dos claves privadas y habiendo recibido, el operador, por parte del Registro Público de Panamá los correspondientes Certificados Electrónicos Calificados de Autenticación de Sitios Web de acuerdo con lo establecido en la Política de Certificación de Certificados de Autenticación de Sitios Web, en la Declaración de Prácticas de Certificación del Registro Público de Panamá y de conformidad con la Ley N° 82 de 2012, "Que otorga al Registro Público de Panamá atribuciones de autoridad registradora y certificadora raíz de firma electrónica para la República de Panamá, modifica la Ley 51 de 2008 y adopta otras disposiciones" y la Ley N° 51 de 2008 "Que define y regula los documentos electrónicos y las firmas electrónicas y la prestación de servicios de almacenamiento tecnológico de documentos y de certificación de firmas electrónicas y adopta otras disposiciones para el desarrollo del comercio electrónico" y sus reglamentos.

Cláusula primera: Condiciones aplicables a los servicios de certificación

Es obligación de los titulares de los certificados electrónicos emitidos bajo la presente licencia de uso:

1. Suministrar información exacta, completa y veraz con relación a los datos que los encargados de su verificación les soliciten para realizar el proceso de registro, responsabilizándose de su veracidad y actualización.
2. Informar a los responsables del Registro Público de Panamá de cualquier modificación de esta información.
3. Custodiar el certificado electrónico y su clave privada, tomando las precauciones requeridas para evitar su pérdida, revelación, modificación o uso no autorizado.

4. Solicitar inmediatamente la suspensión o revocación cuando se cumpla algunos de los supuestos de suspensión o revocación de certificados electrónicos, previstos en la Ley, DPC y en la Política de Certificación aplicable al perfil de certificado electrónico, entre ellos:
 - a. Confirmación de que alguna información o hecho contenido en el certificado electrónico calificado es falso, así como la ocurrencia de hechos nuevos que provoquen que los datos originales no se adecuen a la realidad,
 - a. Conocimiento o sospecha del compromiso de la seguridad de la clave privada correspondiente a la clave pública del certificado.
 - b. Otras causas como: pérdida, robo, compromiso potencial, divulgación, conocimiento por terceros del PIN y/o PUK, que conlleven a su uso no autorizado.

De no hacerlo, el titular del Certificado conoce que según la Ley es responsable por las pérdidas o perjuicios en los cuales incurran terceros de buena fe que confiaron en el contenido del certificado electrónico.

5. Mantener bajo su exclusivo conocimiento el código PIN y PUK.
6. Conocer y aceptar las condiciones de utilización de los certificados electrónicos, en particular de las contenidas en la DPC y en la política de certificación aplicable al perfil de certificado electrónico, así como de las modificaciones de estas.
7. Limitar y adecuar el uso del certificado electrónico al ámbito estipulado en la DPC, la política de certificación aplicable al perfil y a cualquier límite fijado en el propio Certificado Electrónico.
8. No alterar, manipular, monitorizar o realizar actos de ingeniería inversa sobre la implantación técnica (hardware y software) de los servicios, infraestructura y certificados electrónicos que se le han entregado.
9. Utilizar el Certificado conforme a la Ley y a los límites fijados por la DPC y el propio Certificado según su perfil, esto implica que no debe transferir ni delegar a un tercero sus responsabilidades sobre un certificado electrónico que se le haya asignado.
10. Cualquier otra que se derive de la ley, su reglamentación, del contenido de la DPC o de la Política de Certificación aplicable.

Cláusula segunda: Vigencia de los certificados electrónicos:

El periodo de vigencia de los certificados electrónicos entregados bajo el presente acuerdo será de dos años, contados a partir de la fecha y hora de su emisión y concluye cuando haya pasado el tiempo de vigencia que se encuentra en el propio certificado electrónico.

Cláusula tercera: Renovación de los certificados electrónicos:

La renovación de los certificados únicamente debe ser solicitada por el titular en los canales de solicitud establecidos por la Dirección Nacional de Firma Electrónica, cuando se encuentre próximo a vencer el certificado y cuando desee continuar utilizándolo.

Previo a la fecha de caducidad del certificado, el suscriptor recibirá una notificación de recordatorio del vencimiento, que será enviada a la dirección de correo electrónico suministrada durante la emisión del certificado, sin embargo, no es obligación de la Dirección Nacional de Firma Electrónica (DNFE) garantizar la efectividad de la notificación sobre la terminación de la vigencia de su certificado electrónico o confirmar la recepción de la misma, pues es una obligación del suscriptor, conocer la vigencia de su certificado electrónico y adelantar los trámites pertinentes ante la DNFE para la emisión de su nueva firma electrónica.

Cláusula cuarta: Revocación de los certificados electrónicos:

La revocación del certificado electrónico únicamente la puede realizar el titular del certificado o la DNFE cuando se tenga conocimiento o sospecha de compromiso de la clave del titular o cualquier otro hecho determinante que recomendara emprender dicha acción. La solicitud de revocación la debe realizar a través de correo electrónico a servicios@firmaelectronica.gob.pa.pa, adjuntando una nota formal de solicitud y firmado con su firma electrónica u hológrafa, esta última debe coincidir con su firma registrada en su documento de identidad personal o de manera presencial, en las instalaciones de la DNFE de lunes a viernes en el horario de 8:00 am a 04:00 pm (días hábiles), entregando una nota de solicitud formal y presentando su documento de identidad personal.

Clausula quinta: Resolución de quejas:

Todas reclamaciones entre usuarios y la PKI del REGISTRO PUBLICO DE PANAMA (RPP-PKI) deberán ser comunicadas a la DNFE con el fin de intentar resolverlo entre las mismas partes. El usuario podrá remitir sus inquietudes o quejas sobre el servicio a la dirección <https://www.firmaelectronica.gob.pa/contactenos.html> las cuales serán resueltas de en un término máximo de 30 días. En el caso de que no se llegue a un acuerdo entre las partes, la resolución de cualquier conflicto que pudiera surgir se someterá luego de agotada la vía gubernativa al tribunal contencioso administrativo correspondiente.

Cláusula sexta: Protección de datos:

El suscriptor acepta mediante el presente documento proveer al prestador de servicios de certificación de la información que este requiera para cumplir las finalidades del tratamiento de datos relacionadas al ciclo de vida del certificado electrónico.

Las finalidades de tratamiento de datos relativos al servicio de certificación son:

1. Comprobación de identidad de los suscriptores y/o firmantes de los certificados electrónicos calificados.
2. Emisión y gestión de certificados electrónicos calificados.
3. Gestión del ciclo de vida del certificado que incluye: suspensión, renovación, reactivación y revocación.
4. Comunicaciones relativas al servicio.
5. Custodia y mantenimiento del archivo relativo al certificado electrónico calificado.
6. Gestión administrativa derivada del servicio.

El prestador de servicios de certificación garantiza la protección, la confidencialidad y el debido uso de la información suministrada por el suscriptor al prestador de servicios de certificación de conformidad con el artículo 23 numeral 11 de la Ley 51 de 2008 modificada por la ley 82 de 2012 limitando su empleo a las necesidades propias del servicio de certificación descritas en el párrafo anterior, salvo orden de los tribunales competentes, legislación que así lo establezca o a pedido del titular o suscriptor del certificado electrónico. Para que esta garantía aplique es indispensable que el suscriptor brinde información veraz al prestador de servicio de certificación y que el prestador de servicios de certificación haya podido comprobar la veracidad de dicha información.

El responsable de la custodia de la información del suscriptor requerida mediante el presente documento es la Dirección Nacional de Firma Electrónica del Registro Público de Panamá.

El presente acuerdo cumple con la normativa especial de confidencialidad previsto en la Ley 51 de 2008 (Ley de Firma Electrónica), Ley 82 de 2012 (Ley de Firma Electrónica), Ley 81 de 2019 (Ley de protección de Datos Personales), Decreto Ejecutivo 285 de 2021 (Reglamento de la Ley de Protección de Datos Personales) y demás normas que los modifiquen, adicionen, complementen o desarrollen.

Cláusula séptima: Tiempo de archivo de las evidencias:

Se conservará registrada, toda información y documentación relativa a la generación, suspensión y revocación de un certificado electrónico calificado, incluyendo la información suministrada por el suscriptor, así como las declaraciones de prácticas de certificación vigentes de cada momento, con un mínimo de siete (7) años contados desde el momento de la emisión del certificado electrónico de conformidad con el artículo 23 numeral 15 Ley 51 2008 modificada por la Ley 82 de 2012.

Clausula octava: Ley aplicable y jurisdicción:

La ley y jurisdicción de la República de Panamá es la aplicable a la presente Licencia de Uso / Documento de Aceptación de Condiciones de acuerdo con la Ley 51 de 2008 modificada por la Ley 82 de 2012.

Cláusula novena: Excepción de responsabilidad:

La RPP-PKI solo responderá en el caso de incumplimiento de las obligaciones contenidas en la Ley 82 de 2012 y la Ley 51 de 2008, en la presente DPC y en las Políticas de Certificación específicas.

La RPP-PKI sólo responderá de los daños y perjuicios causados por el uso indebido del certificado, cuando se haya consignado en él o en su Política de Certificación asociada, de forma claramente reconocible por terceros, el límite en cuanto a su posible uso o al importe del valor de las transacciones válidas que pueden realizarse empleándolo.

La RPP-PKI, como Prestador de Servicios de Certificación, no se responsabiliza del contenido de los documentos firmados con sus certificados, ni de cualquier otro uso de sus certificados, como pueden ser procesos de cifrado de mensajes de datos o comunicaciones.

La RPP-PKI no representa en forma alguna a los usuarios ni a terceras partes aceptantes de los certificados que emite.

La RPP-PKI no asume ninguna responsabilidad en caso de cualquier tipo de pérdida o perjuicio:

- De los servicios que presta, en caso de guerra, catástrofes naturales o cualquier otro supuesto de caso fortuito o de fuerza mayor: alteraciones de orden público, huelga en los transportes, corte de suministro eléctrico y/o telefónico, virus informáticos, deficiencias en los servicios de telecomunicaciones o el compromiso de las claves asimétricas derivado de un riesgo tecnológico imprevisible.
- Ocasionados durante el periodo comprendido entre la solicitud de un certificado y su entrega al usuario.
- Ocasionados durante el periodo comprendido entre la revocación de un certificado y el momento de publicación de la siguiente CRL.
- Ocasionados por el uso de certificados que exceda los límites establecidos por los mismos, la Política de Certificación pertinente y la Declaración de Prácticas de Certificación (DPC).
- Ocasionados por el mal uso de la información contenida en el certificado.
- Ocasionado por el uso indebido o fraudulento de los certificados o CRLs emitidos por RPP-PKI.
- RPP-PKI no asumirá responsabilidad alguna en relación con el uso de los Certificados emitidos por sus CAs y el par de claves privada/pública asociado a sus titulares para cualquier actividad no especificada en la DPC o en las Políticas de Certificación correspondientes.
- RPP-PKI, como Prestador de Servicios de Certificación, no será responsable del contenido de los documentos electrónicos, ni mensajes de datos firmados con sus certificados ni de cualquier otro uso de sus certificados, como pueden ser procesos de cifrado o comunicaciones.

Cláusula décima: Comunicaciones:

Dirección Nacional de Firma Electrónica

Avenida Samuel Lewis, Frente a la Fiscalía General de Cuentas, Edificio Firma Electrónica, Bella Vista, Campo Alegre, Ciudad de Panamá.

<https://www.firmaelectronica.gob.pa/>

<http://pki.gob.pa/>

Contacto: servicios@firmaelectronica.gob.pa

Clausula decimoprimer: Vigencia:

El presente acuerdo entrará en vigor a partir de su firma, por la que se tiene por demostrado que el suscriptor aceptó y declara conocer los términos y condiciones previstos en la Ley, DPC y en la Política de Certificación aplicable al perfil de certificado electrónico.

Cláusula decimosegunda: Aceptación de Condiciones

El solicitante, acepta las condiciones de uso establecidas en la DPC, así como de la Política de Certificación correspondiente al **Certificado de Autenticación de Sitios Web**, que se encuentra publicada en el portal web <http://www.pki.gob.pa/normativa/index.html> y es de total conocimiento por el solo hecho de haber solicitado la emisión de un certificado electrónico; asimismo, se compromete a cumplir con las obligaciones descritas en estos y que en síntesis se recogen en el presente documento.

Declaro que como solicitante he recibido los certificados electrónicos de autenticación y firma, emitidos por la infraestructura de Clave Pública del Registro Público de Panamá a mi nombre, he sido informado del contenido del presente documento, por lo que acepto cumplir con las obligaciones inherentes a la posesión y uso de los certificados electrónicos calificados.

Nombre y firma del Titular de los Certificados
Electrónicos Calificados de Autenticación de
Sitios Web

Nombre y firma de la persona que valida la
identidad del Titular de los Certificados de
Autenticación de Sitios Web
