# REGLAMENTO INTERNO DE USO DE LA FIRMA DIGITAL DE LA PROCURADURÍA GENERAL DEL ESTADO

Contenido



## TÍTULO I
## GENERALIDADES

### CAPÍTULO I
### DISPOSICIONES GENERALES

Artículo 1°. - (Objeto). El presente Reglamento tiene por objeto, Reglamentar el uso de la firma digital en los documentos digitales, correo institucional y sistemas de información de la Procuraduría General del Estado (PGE) que requieran ser firmados digitalmente.

Artículo 2°. - (Ámbito de Aplicación). El presente Reglamento es de cumplimiento y de aplicación obligatoria para servidores públicos autorizados para el uso de la firma digital de la PGE.

Artículo 3°. - (Marco Normativo). El Reglamento para el Uso de la Firma Digital, tiene como marco normativo las siguientes disposiciones legales:

1. Constitución Política del Estado Plurinacional de Bolivia.
2. Ley N° 064 "Ley de la Procuraduría General del Estado" con las modificaciones e incorporaciones establecidas en la Ley N° 768 de 15 de diciembre de 2015.
3. Ley Nº 164, de 8 de agosto de 2011, Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación.
4. Decreto Supremo Nº·1793, de 13 de noviembre de 2013, que aprueba el Reglamento a la Ley Nº 164, de 8 de agosto de 2011 para el Desarrollo de Tecnologías de Información y Comunicación.
5. Decreto Supremo Nº 3527 de 11 de abril de 2018, que modifica parcialmente el Decreto Supremo Nº 1793, en lo referido a Certificados Digitales y Niveles de Seguridad.
6. Decreto Supremo N° 28168 del 17 de mayo del 2005 de Acceso a la Información.
7. Resolución Ministerial Nº 235, del Ministerio de la Presidencia, de 21 de agosto de 2018, que aprueba el Reglamento para normar el uso de la Firma Digital respecto a niveles de seguridad.
8. Declaración de Prácticas de Certificación y Políticas de Certificación de la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB).
9. Resolución Procuraduríal 054/2021 de 1 de julio de 2021 que aprueba el Plan de Desarrollo Tecnológico de la PGE.
10. Otras disposiciones legales vigentes.

Artículo 4°. – (Principios de la Firma Digital). Los documentos con firma digital se rigen por los siguientes principios:

1. Autenticidad: La información del documento digital y su firma digital corresponden con la persona que ha firmado, puesto que la firma digital permite verificar la identidad del signatario de un documento.
2. Integridad: Un documento firmado digitalmente no ha sido alterado en el proceso de transmisión desde su firma por parte del emisor hasta su recepción por el destinatario.
3. No repudio: Garantía de que un mensaje electrónico de datos o un documento digital ambos firmados digitalmente, no pueden ser negados en su autoría y contenido.

Artículo 5°. - (Uso de la Firma Digital). Las autoridades señaladas a continuación podrán solicitar la emisión de un certificado digital y utilizar la firma digital en documentos de la PGE:

i. Procurador General del Estado.
ii. Subprocuradores.
iii. Director de la Escuela de Abogados.

Otros niveles que podrán solicitar este servicio son:

i. Directores de las Áreas Sustantivas.
ii. Otro personal autorizado por la MAE.

Artículo 6°. - (Definiciones). Para el cumplimiento del presente Reglamento, se deberán considerar las siguientes definiciones:

1. **Certificado Digital:** Es un documento digital firmado digitalmente por una entidad certificadora autorizada que vincula los datos de verificación de firma a un signatario y confirma su identidad. El Certificado Digital es válido únicamente dentro del período de vigencia indicado en el mismo.
2. **Documento digital:** Es toda representación digital de actos, hechos o datos jurídicamente relevantes, con independencia del soporte utilizado para su fijación, almacenamiento o archivo.
3. **Documento digital firmado digitalmente:** Documento digital al cual se le ha aplicado el método criptográfico asimétrico de generación de firma digital.
4. Firma digital: Es la firma electrónica que identifica únicamente a su titular, creada por métodos que se encuentren bajo el absoluto y exclusivo control de su titular, susceptible de verificación y está vinculada a los datos del documento digital de modo tal que cualquier modificación de los mismos ponga en evidencia su alteración.
5. **Firma electrónica:** Es el conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario

como su medio de identificación, que carece de alguno de los requisitos legales para ser considerada firma digital.

6. **Firma digital automática:** Firma digital generada por un sistema informático, donde el titular del certificado digital delega su uso a sistemas determinados para tareas definidas en éste.
7. **TOKEN Físico:** Dispositivo físico electrónico criptográfico que almacena contraseñas y certificados digitales llevando la identidad digital de la persona y que permite al titular de la firma digital poder inscribir la misma en documentos digitales.
8. **Soft -TOKEN:** Software que almacena contraseñas y certificados digitales llevando la identidad digital de la persona y que permite al titular de la firma digital poder inscribir la misma en documentos digitales.
9. **Masiva:** Se entiende por masiva a la gestión de cinco o más certificados digitales, en otro caso se considera como casos individuales.
10. **Administrador:** Persona jurídica de la PGE.
11. **Autenticación:** Proceso tecnológico de verificación por el cual se garantiza la identidad del signatario en un mensaje electrónico de datos o documento digital, que contenga firma digital.
12. **Clave privada:** Conjunto de caracteres alfanuméricos generados mediante un sistema de cifrado que contiene datos únicos que el signatario emplea en la generación de una firma digital sobre un mensaje electrónico de datos o documento digital.
13. **Clave pública:** Conjunto de caracteres de conocimiento público, generados mediante el mismo sistema de cifrado de la clave privada; contiene datos únicos que permiten verificar la firma digital del signatario en el certificado digital.
14. **Criptografía asimétrica:** Conjunto de técnicas que consisten en el uso de las claves privada y pública para cifrar y descifrar la información, aplicada a los datos para asegurar su confidencialidad, integridad y autenticidad.
15. **Huella de Identificación (Hash):** Es el resultado de aplicar algoritmos matemáticos al documento digital, para transformarlo en una cadena de caracteres de longitud fija, asociado unívocamente a los datos del documento digital original.
16. **Entidad de Certificación:** Entidad que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital. Asimismo, puede asumir las funciones de registro o verificación.
17. **Entidad de Certificación Extranjera:** La que no se encuentra domiciliada en el país, ni inscrita en los Registros Públicos de Bolivia, conforme a la legislación de la materia.
18. **Estándares Técnicos Internacionales:** Requisitos de orden técnico y de uso internacional que deben observarse en las Prácticas de Certificación para garantizar el intercambio de claves públicas y la emisión de firmas y certificados digitales, mediante criptografía asimétrica.

19. **Reconocimiento:** Proceso a través del cual la autoridad administrativa competente, equipara y reconoce oficialmente a las entidades de certificación extranjeras.
20. **Integridad:** Característica única del mensaje electrónico de datos o documento digital ambos con firma digital, que indica que los mismos no han sido alterados en el proceso de transmisión desde su creación por parte del emisor hasta la recepción por el destinatario.
21. **Mensaje electrónico de datos:** Toda información de texto, imagen, voz, video y datos codificados digitalmente, creada, generada, procesada, enviada, recibida, comunicada o archivada por medios electrónicos, que pueden ser transmitidos por cualquier sistema de comunicación electrónico.
22. **No Repudio:** Garantía de que un mensaje electrónico de datos o un documento digital ambos firmados digitalmente, no puedan ser negados en su autoría y contenido.
23. **Solicitante:** Persona natural o jurídica que solicita se le emita un certificado digital.
24. Sistema informático: Sistema compuesto de equipos y personal pertinente que realiza funciones de entrada, proceso, almacenamiento, salida y control con el fin de llevar a cabo una secuencia de operaciones con datos.
25. **Destinatario:** Persona designada por el iniciador para recibir un mensaje de datos o un documento electrónico, siempre y cuando no actúe a título de intermediario.
26. **Titular de certificado digital o Signatario:** Persona natural o jurídica a quien se le atribuye de manera exclusiva un certificado digital que le permite firmar digitalmente. Quién se adhiere como signatario al cumplimiento de un contrato y a los términos y condiciones para la provisión de servicios de certificación digital emitidos por la ADSIB.
27. **Titular de firma digital:** Persona natural a quien se le vincula de manera exclusiva con un mensaje de datos firmado digitalmente utilizando su clave privada. Por excepción, en el caso de firmas digitales generadas a través de agentes automatizados, se considera titular de la firma digital a la persona natural o jurídica titular del certificado digital a partir del cual se generan dichas firmas digitales.
28. **Usuario:** Personal registrado que cuenta con un identificador y una clave de acceso para hacer uso de un servicio de la firma digital.
29. **Presunción de autoría y responsabilidad:** Para efectos legales y administrativos, todos los documentos firmados digitalmente contarán con la responsabilidad y autoría de los usuarios.
30. **Revocación:** Es el acto por el cual se invalida un certificado digital antes de su caducidad.
31. **Rectificar:** Subsanar de los defectos de un documento firmado digitalmente en su contenido.

Artículo 7°. - (Abreviaciones). Para el cumplimiento del presente Reglamento, se deberán considerar las siguientes abreviaciones:

1. Procuraduría General del Estado: PGE
2. Agencia para el Desarrollo de la Sociedad de la Información en Bolivia: ADSIB
3. Huella de Identificación: HASH
4. Máxima Autoridad Ejecutiva: MAE
5. Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes: ATT
6. Unidad de Tecnologías de la Información y Comunicación: UTIC
7. Servicio General de Identificación Personal: SEGIP
8. Solicitante de Firma de Certificado: CSR
9. Responsable de seguridad de la Información: RSI

## TÍTULO II
## DE LA FIRMA DIGITAL

### CAPÍTULO I
### FINALIDAD DE LA FIRMA DIGITAL

Artículo 8°. - (Finalidad de la Firma Digital). La firma digital tiene por finalidad dar seguridad y validéz legal al documento digital, correo institucional o sistemas de información, enviado por el signatario, garantizando:

1. Que el documento digital fue firmado digitalmente por el signatario (autenticación).
2. Que el documento digital no ha sufrido alteraciones durante su transmisión (integridad).
3. Que el signatario no pueda desconocer un documento digital que ha sido firmado usando su clave privada (no repudio).

### CAPÍTULO II
### CARACTERISTICAS DE LA FIRMA DIGITAL

Artículo 9°. - (Características de la Firma Digital). La firma digital, para ser usada en la PGE, debe poseer las características mínimas siguientes:

1. Al momento de su creación, los datos con los que es creada deben estar bajo control exclusivo del signatario.
2. Debe permitir verificar unívocamente la autoría e identidad del signatario, mediante dispositivos tecnológicos de comprobación.
3. Debe ser única para cada documento digital firmado digitalmente.
4. Debe ser susceptible de verificación, usando la clave pública del signatario.

5. Debe estar vinculada a un certificado digital de manera que cualquier alteración subsiguiente en el mismo, sea detectable.
6. Estar vinculada a un certificado digital de manera que, cualquier alteración subsiguiente en el mismo sea detectable.
7. Haber sido creada durante el periodo de vigencia del certificado digital válido del firmante.
8. Haber sido creada utilizando un dispositivo de creación de firma tecnológicamente seguro y confiable.
9. Ser creada por medios que el firmante pueda mantener bajo su exclusivo control y la firma sea controlada por la persona a quien pertenece.
10. Contener información vinculada exclusivamente a su titular.
11. Permitir verificar unívocamente la autoría e identidad del signatario, mediante dispositivos tecnológicos de comprobación, de tal manera que es posible detectar si la firma digital o el mensaje de datos ha sido alterado.
12. Que el método de creación y verificación sea confiable, seguro e inalterable para el propósito para el cual fue generado un registro de creación de la firma.
13. Que los datos sean susceptibles de verificación por terceros.
14. Que, al momento de creación de la firma digital, los datos con los que se creare, se hallen bajo control exclusivo del signatario.
15. Los documentos generados con el uso de la firma digital, deberán ser recepcionados y procesados de manera obligatoria en entidades públicas y privadas, en cumplimiento al DS. 3525 art. 14.
16. Los documentos adjuntos en el correo electrónico oficial firmado digitalmente, sea cual fuere su formato, forman parte indivisible del documento enviado, de lo contrario pierden su valor legal.
17. La firma digital en las plataformas de Android, IPhone y otras están sujetas al soporte y recomendaciones de la ADSIB.

## TÍTULO III
## SUJETOS DE LA RELACIÓN JURÍDICA Y EFECTOS LEGALES

### CAPÍTULO I
### SUJETOS DE LA RELACIÓN JURÍDICA Y VALIDÉZ PROBATORIA DE LA FIRMA DIGITAL

Artículo 10°. - (Relación Jurídica). Para efectos del presente Reglamento, se entiende por relación jurídica al vínculo existente entre el Titular del Certificado Digital, la Entidad Certificadora autorizada y la PGE.

1. La relación jurídica para uso de la Firma Digital, se inicia con la solicitud de emisión del Certificado Digital y firma de contrato entre el Titular del Certificado

Digital y la Entidad Certificadora y concluye con la revocación o conclusión de la vigencia del Certificado Digital.

2. La conclusión de la relación jurídica, no implica el cese o extinción de las obligaciones o responsabilidades del Titular del Certificado Digital, emergentes de acciones, actos u omisiones realizados durante el período de vigencia del Certificado Digital.

Artículo 11°. - (Uso de la Firma Digital). La Firma Digital, permite realizar la gestión Integra de la documentación que produce la PGE en medios digitales, de la misma manera cuenta con un dispositivo criptográfico (TOKEN) de nivel de seguridad alto que almacena el Certificado Digital, que permite realizar la firma en los documentos digitalmente.

## CAPÍTULO II
## VALIDÉZ PROBATORIA, REVOCATORIA, RECTIFICACION E INVALIDÉZ DE DOCUMENTOS DIGITALES

Artículo 12°. - (**Validéz Jurídica y Probatoria de Documentos Digitales Firmados Digitalmente**). Los documentos emitidos por firma digital de la PGE poseen plena Validéz jurídica y probatoria conforme lo establecido en el artículo 78 de la Ley N° 164 - Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación de 08 de agosto de 2011.

Artículo 13°. – **(Documentos Firmados Digitalmente**). Como medio de prueba Las firmas digitales, así como los mensajes de datos y documentos firmados digitalmente podrán ser admitidas como prueba en toda clase de procesos o procedimientos. El Juez podrá solicitar a la autoridad administrativa competente el nombramiento de un perito especializado en firmas digitales.

Artículo 14°. – **(Presunciones acerca de las firmas electrónicas bajo la Infraestructura Oficial).** Tratándose de mensaje de datos o documentos firmados electrónicamente con firmas generadas bajo la Infraestructura Oficial de Firma Electrónica, se presume que el documento o mensaje de datos fue enviado y firmado por su titular, de manera tal que identifica y vincula al firmante, y presume la autenticación e integridad del mismo.

Las disposiciones y presunciones del Reglamento no excluyen el cumplimiento de las formalidades específicas requeridas para los actos jurídicos y el otorgamiento de fe pública.

Artículo 15°. - (Revocatoria del Certificado Digital). La revocación del certificado digital procederá en los siguientes casos:

1. Revocación a solicitud expresa del usuario. El Titular del Certificado Digital podrá solicitar la revocación mientras el mismo se encuentre vigente, en caso de la pérdida del dispositivo TOKEN y/o que su clave privada haya estado comprometida en algún caso. En este sentido, el titular deberá solicitar inmediatamente la revocación del certificado digital a través de la INTRANET de la PGE, especificando el motivo de su solicitud. Para obtener un nuevo certificado, se deberá solicitar la reemisión del certificado digital.
2. Revocación por no firma del Contrato de Adhesión. El certificado digital será revocado de forma automática al vencimiento del plazo establecido por la ADSIB, sin que el titular del mismo hubiese firmado el Contrato de Adhesión para la prestación de Servicios de Certificación digital. Para obtener un nuevo certificado, se deberá solicitar la reemisión del certificado digital.
3. Cuando la confidencialidad de la clave privada ha sido puesta en duda o exista riesgo de un uso indebido.
4. Cuando la clave privada ha sido eliminada, destruida o es inaccesible.
5. Cuando la MAE deja sin efecto los poderes conferidos al signatario.
6. Por orden judicial o de autoridad administrativa competente.
7. Por fallecimiento del titular del certificado.
8. Por incumplimiento de las causas pactadas entre la entidad certificadora con el titular del certificado digital.
9. Por disolución de la persona jurídica.
10. Otros establecidos en la Reglamentación específica emitida por la ATT.
11. Por el cese de operaciones de la entidad de certificación que lo emitió.
12. Otras causales que establezca la autoridad administrativa competente.

Artículo 16°. - (**Rectificación de documentos con firma digital**). Los documentos sujetos de rectificación, pueden ser subsanados de sus defectos, previo informe que justifique la modificación o anulación del documento original y sea conforme a procedimiento que establezca la ADSIB.

Artículo 17°. - (**Invalidéz de la Firma Digital**). - Está sujeta a los siguientes casos:

1. En fines distintos para el que fue extendido el certificado digital.
2. Cuando el certificado haya sido cancelado al cese de funciones.
3. Cuando la vigencia de la firma digital haya terminado.

## CAPÍTULO III
## RECONOCIMIENTO POR PARTE DE LA PGE DE LOS DOCUMENTOS EXTERNOS FIRMADOS DIGITALMENTE

Artículo 18°. – (Reconocimiento de documentos externos). La PGE reconoce todos los documentos que provengan de los emisores con firma digital, siempre y cuando estos cumplan con los parámetros establecidos por la entidad certificadora.

# TÍTULO IV
# FIRMA Y CERTIFICADO DIGITAL

## CAPÍTULO I
## FIRMA DIGITAL

Artículo 19°. – (Uso de la Firma Digital). Los documentos digitales establecidos en el Art. 58 del presente Reglamento, el correo institucional (de uso interno y externo) y los sistemas de información de la PGE en los que se ha dispuesto oficialmente la aplicación de la firma digital, deberán ser firmados digitalmente por el Titular del Certificado Digital.

Artículo 20°. – (Aplicación de la Firma Digital en Los documentos digitales, correo institucional y sistemas de información de la PGE). La solicitud de la firma digital para los documentos producidos en esta institución, deberán ser autorizados por la MAE y ser canalizados por la DGAA y la UTIC en el marco de sus competencias y atribuciones.

Artículo 21°. – (El Servidor Público Autorizado para el Uso de la Firma Digital). Este tiene las siguientes obligaciones:

1. Firmar los documentos para este fin, este deberá ser habilitado para el uso de la firma digital en documentos inherentes a sus atribuciones y competencias.
2. Cumplir con las condiciones y requisitos establecidos en el presente Reglamento, otros documentos normativos que emita la PGE, y reglamentación externa del órgano rector para el uso de la firma digital.

Artículo 22°. - (Tipos de Firma Digital). La PGE aprobará a través de la UTIC, la utilización del tipo de firma digital (por software o físico) en función al costo, facilidad de uso y otras variables que considere necesarias.

Artículo 23°. – (Estándares aplicables bajo la Infraestructura Oficial de Firma Digital). Las prácticas de certificación comprendidas en la Infraestructura Oficial de Firma Digital deben estar basadas sobre los estándares tecnológicos internacionales vigentes, que aseguren la interoperabilidad, las funciones exigidas en la Ley 164 y sus Decretos Supremos Reglamentarios. La autoridad administrativa competente determinará los estándares compatibles aplicando el principio de soberanía tecnológica.

## CAPÍTULO II

## CERTIFICADO DIGITAL

Artículo 24°. - (Certificado Digital). Es emitido por la ADSIB como Entidad Certificadora Pública, bajo los Reglamentos y procedimientos establecidos por dicha entidad.

Artículo 25°. - (Características del Certificado Digital). En cumplimiento a la Ley N° 164 de Telecomunicaciones y Tecnologías de la Información y Comunicación y su reglamentación, el certificado digital deberá cumplir con los siguientes requisitos:

1. La emisión debe ser realizada por una entidad de certificación autorizada por la ATT o ser reconocida por una entidad certificadora autorizada nacional.
2. Contener el número único de serie que identifica el certificado.
3. Responder a formatos estándares reconocidos internacionalmente.
4. Exponer su periodo de validez.
5. Ser susceptibles de verificación respecto de su estado de revocación.
6. Acreditar, en los supuestos de representación, las facultades del signatario para actuar en nombre de la persona jurídica a la que represente.
7. Contemplar la información necesaria para la verificación de la firma.
8. Identificar la política de certificación bajo la cual fue emitido.
9. Contemplar las características técnicas y los límites de uso del certificado.
10. Validar la correspondencia jurídica entre el certificado digital, la firma digital y la persona.
11. Identificar inequívocamente a su titular y al certificador autorizado que lo emitió.
12. Identificar su nivel de seguridad, en caso que el par de claves sea generado por dispositivo, éste tendrá nivel de seguridad alto, en caso que el par de claves sea generado por software éste tendrá nivel de seguridad normal.
13. A efectos de la validación de la firma digital del signatario se hará uso de la dirección web: validar.firmadigital.bo o en su defecto, mediante la herramienta JACOBITUS accesible mediante un equipo local.

# TÍTULO V

# CERTIFICADORAS Y VIGENCIA DE LA FIRMA DIGITAL

## CAPÍTULO I

## ENTIDADES DE CERTIFICACIÓN

Artículo 26°. - (Entidad Certificadora). La Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB), en su calidad de Entidad Certificadora pública u otras entidades privadas autorizadas por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT), se constituyen en la Entidad Certificadora que emite, valida, renueva, deniega, suspende o da de baja los Certificados Digitales de

conformidad al inciso a), artículo 39 del Reglamento a la Ley N° 164 para el Desarrollo de las Tecnologías de Información y Comunicación aprobado mediante Decreto Supremo N° 1793 de 13 de noviembre de 2013.

Artículo 27°. - (Requisitos de la Entidad de Certificación). La Entidad de Certificación, deberá:

1. Contar con la autorización otorgada por la ATT o en el caso de entidades certificadoras extranjeras, que los certificados digitales sean reconocidos por una entidad certificadora autorizada nacional que garantice, en la misma forma que lo hace con sus propios certificados, el cumplimiento de los requisitos, el procedimiento, así como la validez y vigencia del certificado.
2. Cumplir con los requisitos y condiciones determinados en los Estándares Tecnológicos y otros Lineamientos establecidos para el Funcionamiento de las Entidades Certificadoras, emitidos por la ATT.
3. Contar con normas y prácticas definidas en un manual de operaciones o documento equivalente, que incluya:
    a) Los procedimientos para la generación del certificado y la conservación de registros.
    b) Los procedimientos de acceso a información para los administradores, participantes y signatarios.
    c) Las normas y procedimientos relacionados con el ciclo de vida del certificado.

4. Proporcionar los medios necesarios para posibilitar la revocatoria oportuna del certificado digital.

5. Asegurar al receptor de los documentos digitales firmados digitalmente el acceso a los medios necesarios que le permitan verificar:

    a) La identidad del participante y del signatario a través del certificado digital.
    b) Cualquier limitación del certificado digital.
    c) La validéz del certificado digital.
    d) Cualquier limitación del alcance o del grado de responsabilidad establecido por el certificador.

## CAPÍTULO II
## VIGENCIA DE LOS CERTIFICADOS

Artículo 28°. - (Vigencia del Certificado Digital). El certificado digital estará vigente hasta la fecha de expiración indicada en el mismo. En ningún caso la vigencia podrá ser superior a un (1) año, y no deberá exceder el tiempo de duración de dicho cargo público a menos que exista prorrogas de funciones en la entidad, debiendo comunicar a la ADSIB de manera inmediata.

Artículo 29°. - (Certificados Digitales para generación de Firma Digital Automática).

I. Los certificados digitales con seguridad alta o normal podrán ser usados para realizar la firma digital automática, siempre y cuando la firma la realice en condiciones tecnológicamente seguras y confiables, que eviten su uso por terceros no autorizados.

II. Para la realización del firmado digital de forma automática, se debe comprobar que los datos con los que se creare, sean controlados por medios que permitan evitar de forma tecnológicamente segura y confiable su uso por terceros no autorizados, para otros fines que no se encuentren descritos en el certificado digital.

## TÍTULO VI
## DERECHOS, RESPONSABILIDADES Y PROHIBICIONES POR EL USO DE LA FIRMA DIGITAL

### CAPÍTULO I
### DERECHOS DEL TITULAR DEL CERTIFICADO DIGITAL, RESPONSABILIDADES Y OBLIGACIONES

ARTÍCULO 30°. - (Derechos del Titular del Certificado Digital). El Titular del Certificado Digital tiene los derechos establecidos en el artículo 54 del Reglamento a la ley Nº 164 para el Desarrollo de Tecnologías de Información y Comunicación aprobado mediante Decreto Supremo N° 1793 de fecha 13 de noviembre de 2013.

Artículo 31°. - (Responsabilidades del titular). El titular de la firma digital es responsable:

1. Por el contenido de los documentos digitales firmados digitalmente y por los efectos que estos generen.
2. Por la información contenida en el certificado digital.
3. Por el uso no autorizado del certificado digital y su clave privada.
4. Por los efectos del uso de la firma digital, cuando no se revoque el certificado digital por las causales definidas en el presente Reglamento.
5. Mantener el control y la reserva de la clave privada bajo su responsabilidad.
6. Observar las condiciones establecidas por la entidad de certificación para la utilización del certificado digital y la generación de firmas digitales.
7. Solicitar de inmediato la cancelación de su certificado digital en caso de que la reserva sobre la clave privada se haya visto comprometida, bajo responsabilidad.
8. Mantener un repositorio de los documentos firmados digitalmente por el tiempo de prescripción de la acción.

ARTÍCULO 32°. – (Obligaciones del Titular del Certificado Digital). Son obligaciones derivadas de la relación laboral establecida en el presente Reglamento:

1. Firmar digitalmente los documentos oficiales y en casos excepcionales, firmar de manera física cuando las limitaciones de orden tecnológico o administrativo así lo requieran.
2. Mantener el control y la reserva del método de creación de su firma digital para evitar el uso no autorizado.
3. No utilizar los datos de creación de firma digital cuando haya expirado el período de Validéz del certificado digital; o la entidad de certificación le notifique la suspensión de su vigencia o la conclusión de su validéz.
4. Cumplir las disposiciones contenidas en el presente Reglamento.
5. El signatario, deberá asegurar que los datos y el mecanismo de creación de firma estén resguardados de manera segura y confidencial a fin de evitar su uso no autorizado.
6. La asignación del dispositivo criptográfico (TOKEN) es de uso estrictamente laboral y al interior de la PGE, el usuario es responsable por los documentos firmados digitalmente con el dispositivo criptográfico.
7. Cualquier documento digital firmado por el dispositivo criptográfico (TOKEN) que no tenga relación con los procedimientos y procesos de la PGE, es de entera responsabilidad del usuario.
8. Efectuar la solicitud del Certificado Digital a la ADSIB a través de los canales correspondientes, proporcionando información fidedigna y susceptible de verificación.
9. Observar las condiciones establecidas por la ADSIB para la utilización del Certificado Digital y la generación de la Firma Digital.
10. Efectuar la actualización de sus datos en la ADSIB de acuerdo a las disposiciones emitidas por esta institución.
11. Notificar oportunamente a la ADSIB cuando los datos de creación de su firma digital hayan sido conocidos por terceros no autorizados y que podrían ser indebidamente utilizados, debiendo, para este caso, solicitar la baja de su Certificado Digital.
12. Gestionar, la revocación del Certificado Digital una vez concluida su relación laboral con la PGE o por transferencia de cargo.
13. Gestionar con la debida anticipación, la renovación del Certificado Digital cuando se requiera.
14. Resguardar y custodiar el TOKEN asignado.
15. Tomar las medidas de seguridad necesarias para mantener los datos de generación de la firma digital bajo su estricto control, evitando la utilización no autorizada del Certificado Digital o TOKEN.

16. Notificar la pérdida del TOKEN de manera inmediata y gestionar la revocación del Certificado Digital, cubriendo el costo de reposición de acuerdo a lo definido por la ADSIB.
17. Efectuar la devolución del TOKEN en condiciones de funcionamiento a la UTIC a la conclusión de su condición de Titular del Certificado Digital, por suspensión temporal o desvinculación de la institución.
18. En caso de entregarse el TOKEN dañado o averiado, no se deberá dar curso a la devolución del mismo, debiendo en este caso el servidor público cancelar el costo del mismo a través de la DGAA.
19. Realizar la devolución del TOKEN en caso de cambio de cargo, si las nuevas funciones no requieran el uso de la firma digital; por el contrario, si sus funciones requieren el uso de firma digital, deberá gestionar ante la ADSIB por medio de la UTIC la revocación y activación del Certificado Digital en el TOKEN de acuerdo al nuevo cargo.
20. Portar el TOKEN que le será entregado por la PGE, para el oportuno uso del mismo en la firma digital.
21. Notificar al Responsable de Seguridad de la Información (RSI) cuando existan indicios que la clave del TOKEN ha sido vulnerada.
22. Realizar la devolución del TOKEN a la UTIC; para su custodia, cuando el Titular del Certificado Digital esté suspendido de forma temporal.
23. En caso de desvinculación del titular del Certificado Digital, debe proceder a la devolución del TOKEN con documentación que respalde la revocación del Certificado Digital (ADSIB), con copia remitida a la UTIC.

## CAPÍTULO IV
## PROHIBICIONES Y SANCIONES DEL TITULAR DEL CERTIFICADO DIGITAL

Artículo· 33°. - (Prohibiciones). Queda terminantemente prohibido para el titular del certificado digital, lo siguiente:

1. Usar la firma digital para beneficio particular o privado.
2. Prestar o transferir el dispositivo criptográfico (TOKEN) a otro usuario (servidores públicos y consultores individuales de línea) para su uso.
3. Enajenar el dispositivo criptográfico (TOKEN) a otro usuario (servidores públicos y consultores) a título oneroso o gratuito.
4. Dañar o alterar sus características físicas o técnicas del dispositivo criptográfico (TOKEN).

Artículo 34°. - (Sanciones)

El incumplimiento u omisión de lo dispuesto por el presente Reglamento dará lugar al inicio acciones administrativas y legales pertinentes a los usuarios autorizados para la firma digital.

## TÍTULO VII
## RESPONSABILIDAD DE LAS UNIDADES DE APOYO

### CAPÍTULO I
### RESPONSABILIDADES DE LA UTIC Y LA DGAA

Artículo 35°. - Responsabilidades de la UTIC:

1. Realizar el seguimiento y monitoreo al cumplimiento del presente Reglamento.
2. Con la información de los servidores públicos autorizados para el uso de la Firma Digital, la UTIC gestionará la remisión de una carta firmada por la MAE, mediante la cual hará conocer a la ADSIB la lista de los servidores públicos que tienen autorización para la obtención y uso de la Firma y el Certificado Digital.
3. Implementar mecanismos para la aplicación de la firma digital en los documentos digitales, correo institucional y sistemas de información de la PGE, determinados para este fin.
4. Brindar soporte tecnológico y capacitación al titular del Certificado Digital y usuarios de los sistemas de información con firma digital.
5. Gestionar la adquisición de los dispositivos TOKEN de acuerdo a la demanda que se genere en función a las aplicaciones implementadas de firma digital y los servidores públicos que requieran hacer uso de la firma digital.
6. Gestionar la recepción, asignación, y entrega de los dispositivos TOKEN.
7. Llevar el registro y controlar las altas y bajas de certificados digitales en la PGE.
8. Revisar periódicamente el presente Reglamento y de ser necesario, proponer su actualización sobre la base del análisis de la experiencia de su aplicación y la dinámica institucional.
9. La UTIC podrá reasignar el TOKEN físico por hasta tres veces durante el periodo de vigencia de la firma digital, en caso de cese de funciones de los titulares, con los costos que disponga la entidad certificadora.
10. La revocación definitiva del Certificado Digital de los funcionarios públicos que no hayan dado de baja este servicio en un tiempo prudente al cese de funciones o reasignación de cargo.

Artículo 36°. - Responsabilidades de la DGAA:

1. Comunicar a la UTIC la desvinculación de los Servidores Públicos que tienen a su cargo una firma digital en la PGE.

2. Acreditar el pago del TOKEN y los derechos de uso de firma digital y certificados digitales, de los usuarios autorizados, adjuntando copia del comprobante de pago.
3. Sí, el Titular del Certificado Digital no presenta el documento de respaldo de la revocación del Certificado Digital, no se otorgará la conformidad ni de la DGAA ni de la UTIC en el Formulario de Dejación de Cargo o Conclusión de Contrato.

## TÍTULO VIII
## CONFIDENCIALIDAD Y OTROS

### CAPÍTULO I
### CONFIDENCIALIDAD

ARTÍCULO 37°. - (Confidencialidad de la Información). La PGE, rige su actuar bajo el principio de confidencialidad de los procesos de interés del Estado, establecidos en el Art. 2 de la Ley 064.

### CAPÍTULO II
### OTROS

Artículo 38°. - (Validación de la Firma Digital) Los procedimientos de validación de la firma digital deberán incluir el uso de certificados digitales emitidos por una Entidad Certificadora Autorizada por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT).

Artículo 39°. - (Tarifa del Servicio de Certificación Digital). la PGE asumirá el costo de la tarifa establecida por la ADSIB para la prestación del servicio de certificación digital de los titulares del Certificado Digital, autorizados para el uso de la firma digital.

Artículo 40°. - (Vigencia y Renovación del Certificado Digital). La vigencia del Certificado Digital será establecida por la ADSIB. Antes de su vencimiento, el Certificado Digital podrá ser renovado por la ADSIB de acuerdo a los reglamentos y procedimientos definidos por esa entidad.

Artículo 41°. - (Dispositivos Criptográficos TOKEN y Certificados Digitales). La PGE podrá adquirir los dispositivos criptográficos (TOKEN) de acuerdo a un costo establecido por la entidad certificadora. Asimismo, se adquirirá los Certificados Digitales en base a los convenios interinstitucionales de intercambio de servicios autorizados, mismas que serán asignadas para uso y custodia de los usuarios servidores públicos autorizados, con la obligación de ser devueltos a la entidad conforme a las previsiones del presente Reglamento.

Artículo 42°. – (Documentos con firma digital masiva). Pueden tener varios firmantes en un mismo documento.

Artículo 43°. – (Convenios entre instituciones en el marco de la cooperación la interoperabilidad). Deberán ser firmados de manera autógrafa por la limitación tecnológica de una de las partes.

## TÍTULO IX
## REVOCACIÓN, SUSPENSIÓN Y REACTIVACIÓN DEL CERTIFICADO DIGITAL

### CAPÍTULO I
### PROCEDIMIENTO

Artículo 44°. – (La revocación, suspensión y reactivación del Certificado Digital). Deberá ser solicitada por el Titular del Certificado Digital ante la ADSIB, de acuerdo a los Reglamentos y Procedimientos definidos por dicha entidad.

Artículo 45°. – (En caso de alguna contingencia). Sí el Titular del Certificado Digital que concluyó su relación laboral con PGE, no cumplió con el proceso de baja del Certificado Digital ante la ADSIB en un término prudente, la UTIC gestionará ante la ADSIB (a través del oficial de registro asignado), la revocación definitiva del Certificado Digital correspondiente.

Artículo 46°. – (Designación de enlaces). El Jefe de Sistemas de la UTIC, designará y actualizará mediante memorándum interno al enlace o los enlaces, para gestionar la firma digital para los funcionarios autorizados de la PGE ante la ADSIB a través de los Oficiales de Registro.

Artículo 47°. - (Requisitos para obtener un certificado digital). Estos deberán ser presentados bajo la formalidad y exigencia de la entidad certificadora.

## TÍTULO X
## ORDEN ADMINISTRATIVO

### CAPÍTULO I
### SOLICITUD DE EMISIÓN DEL CERTIFICADO DIGITAL EN LA PGE

Artículo 48°. - (Formulario de Solicitud). La solicitud de emisión del Certificado Digital deberá ser efectuada a través de la ADSIB.

El solicitante deberá adjuntar al mismo, los siguientes documentos digitalizados:

1. Cédula de Identidad, emitida por el Servicio General de Identificación Personal (SEGIP), original que se encuentre vigente.
2. Correo electrónico institucional.
3. Dirección de su domicilio actual.
4. Número de celular.

De forma previa a registrar el formulario, el solicitante deberá leer y aceptar las Políticas de certificación de la Entidad Certificadora, a fin de tomar conocimiento de los términos y condiciones del servicio prestado. Una vez registrado el formulario, se le asignará un número de solicitud y en el mismo, especificará los pagos que debe realizar la PGE.

El solicitante deberá tomar nota del número de trámite para presentarse posteriormente en el Punto de Registro, una vez que se efectúen los pagos correspondientes.

Artículo 49°. - (Pago por Concepto del Servicio de Certificación Digital). En el caso de los servidores públicos, la PGE deberá realizar el pago de la tarifa establecida por la Entidad Certificadora para la prestación del servicio de certificación digital.

La DGAA deberá acreditar el pago del TOKEN y los derechos de uso de firma digital y certificados digitales, adjuntando copia del comprobante de pago.

Artículo 50°. - (Disponibilidad del TOKEN). Los servidores públicos de la PGE recibirán el TOKEN de forma gratuita, quedando este dispositivo bajo su cargo y custodia en calidad de préstamo mientras dure su vínculo laboral con la PGE.

Artículo 51°. - (Reasignación del TOKEN) El RSI verificará, registrará el número de serie del TOKEN y procederá a la entrega del mismo al solicitante, imprimirá el Acta de Entrega en dos (2) ejemplares que deberán ser suscritos por el RSI y el solicitante. Un ejemplar deberá ser entregado al solicitante como constancia de su entrega y la otra copia para la UTIC, para su posterior reasignación a los servidores públicos autorizados.

Artículo 52°. - (Generación de par de Claves y del CSR). Una vez aprobada la solicitud de emisión del Certificado Digital, el solicitante recibirá un mensaje a través de su correo institucional con la indicación de pasos que debe seguir a fin de generar la clave privada y pública. El solicitante deberá ingresar a la plataforma de solicitud de la ADSIB, conectar su dispositivo TOKEN y activar la firma digital. A partir de la notificación recibida, deberá proceder a la generación del par de claves (privada y pública). El sistema generará de manera automática el CSR.

## CAPÍTULO II
## EMISIÓN DEL CERTIFICADO DIGITAL Y FIRMA DE CONTRATO DE ADHESIÓN

Artículo 53°. - (Emisión del Certificado Digital). La Entidad Certificadora validará y emitirá el Certificado digital en el plazo máximo de setenta y dos (72) horas, salvo que existan observaciones al trámite. Una vez emitido el Certificado Digital, la Entidad Certificadora enviará una notificación al Titular del Certificado Digital a través del correo institucional con las instrucciones para su descarga en el TOKEN.

Artículo 54°. - (Descarga del Certificado Digital en el TOKEN). El Titular del Certificado Digital deberá seguir las instrucciones recibidas para la descarga del Certificado Digital en el Dispositivo TOKEN.

Artículo 55°. - (Firma del Contrato de Adhesión). Una vez descargado el Certificado Digital en el Dispositivo TOKEN, el Titular del Certificado Digital deberá firmar digitalmente el Contrato de Adhesión para la Provisión de Servicios de Certificación Digital en el plazo establecido en la Declaración de Prácticas de Certificación de la ADSIB. En caso que el Titular no firme el contrato en el plazo establecido, el certificado digital será revocado de manera automática y se deberá solicitar la reemisión del mismo.

Artículo 56°. - (Periodo de Validéz del Certificado Digital). El periodo de validéz del Certificado Digital será el que se indique en el propio certificado, como máximo de un (1) año.

El Titular del Certificado Digital deberá verificar la fecha de vigencia de su certificado en el mismo TOKEN o a través de la plataforma de la ADSIB, a fin de realizar las gestiones de renovación o emisión de un nuevo certificado con la debida anticipación a su vencimiento según corresponda.

## CAPÍTULO III
## DEL CERTIFICADO DIGITAL Y REQUISITOS PREVIOS PARA SU EMISION

Artículo 57°. - (Certificado Digital). Los Certificados Digitales utilizados para la firma de documentos de la PGE deberán ser emitidos por la ADSIB en el marco de lo establecido en la Ley N° 164 - Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación de 08 de agosto de 2011, su Reglamento y los procedimientos establecidos por dichas entidades.

## CAPÍTULO IV
## DOCUMENTOS DE USO DE LA FIRMA DIGITAL EN LA PGE

Artículo 58°. - (Documentos de la PGE con Firma Digital). Documentos de la PGE que deberán hacer uso de la firma digital

1. Correo electrónico oficial.
2. Resoluciones Procuraduriales.
3. Recomendaciones Procuraduriales.
4. Requerimientos Procuraduriales.
5. Dictamen Procuradurial.
6. Notas Externas.
7. Notas Internas.
8. Memorándums.

9. Informes de los Subprocuradores y Directores.
10. Minutas de Instrucción.
11. Certificados de la Escuela de Abogados del Estado.
12. Peticiones de Informe Procuraduriales.
13. Sistemas de información de la PGE que se adecuen gradualmente a este mecanismo.
14. Otros documentos de relevancia que considere la MAE.

## CAPÍTULO V
## RENOVACIÓN Y REEMISIÓN DEL CERTIFICADO DIGITAL

Artículo 59°. - (Renovación del Certificado Digital). La renovación del Certificado Digital procederá únicamente cuando la información contenida en éste, no varíe respecto a los datos del certificado emitido inicialmente.

1. La renovación del Certificado Digital para persona jurídica será de una duración máxima de un año. La renovación será responsabilidad del titular y deberá ser realizada a través de la plataforma de la ADSIB.
2. La solicitud de renovación deberá realizarse antes del vencimiento del Certificado Digital, para ello el Titular del Certificado Digital podrá solicitar la renovación del certificado digital treinta (30) días calendario antes de su vencimiento. Una vez que el certificado digital se encuentre vencido, sin que el titular hubiese solicitado la renovación del mismo, el solicitante deberá realizar la solicitud de emisión de un nuevo certificado digital.
3. El titular del Certificado Digital deberá solicitar la renovación a la ADSIB. Para el trámite de renovación no se requiere la presencia física del Titular del Certificado. Una vez emitido el certificado digital se comunicará al Titular para que proceda a la descarga del mismo en el dispositivo TOKEN.
4. La renovación del certificado digital podrá ser solicitada la cantidad de veces establecidas en la Declaración de Políticas de Certificación de la ÁDISIB, sin que sea necesaria la presencia física del titular en la entidad certificadora.

Artículo 60°. - (Reemisión del Certificado Digital). La reemisión del certificado digital procederá cuando el mismo haya sido previamente revocado y siempre que el titular del certificado aún cuente con un periodo de tiempo con el servicio de certificación digital pagado.

## CAPÍTULO VI
## DEL DISPOSITIVO TOKEN

Artículo 61°. - (Uso del TOKEN). Cada Titular del Certificado Digital deberá contar con un TOKEN que cumpla el estándar FIPS140 2, dicho dispositivo podrá ser adquirido por la PGE.

Artículo 62°. - (Desbloqueo del TOKEN). En caso que el dispositivo TOKEN se encuentre bloqueado por ingresar la contraseña o pin de forma incorrecta, el Titular del Certificado Digital deberá solicitar a la ADSIB su desbloqueo.

## CAPÍTULO VII
## ACTUALIZACION Y DIFUSION DEL REGLAMENTO

Artículo 63°. - (Difusión). La UTIC es el responsable de la difusión del presente Reglamento a partir de su aprobación.

## DISPOSICIONES FINALES

Artículo Transitorio 1°. - (Previsiones y Aspectos no Contemplados en el Presente Reglamento)

Los aspectos de orden administrativo no previstos en el presente Reglamento serán resueltos en el marco de la normativa vigente.

En caso de presentarse contradicciones y/o diferencias en la interpretación del presente Reglamento, estos serán solucionados en el marco y previsiones establecidas en las disposiciones legales vigentes que regulan la materia.

Artículo Transitorio 2°. - (Revisión y Actualización del Reglamento)

La UTIC actualizará el Reglamento Interno de Uso de la Firma Digital al menos cada dos años a partir de su aprobación o cuando las circunstancias así lo ameriten en base a un análisis retrospectivo de su aplicación, de acuerdo al funcionamiento de los sistemas y cuando se modifiquen las Normas.