GOBIERNO REGIONAL PUNO

Resolución Ejecutiva Regional

Nº 342 -2022-GR-GR PUNO

PUNO, 18 JUL. 2022

EL GOBERNADOR REGIONAL DEL GOBIERNO REGIONAL PUNO

Vistos, el expediente N° 4905-2022-GGR, sobre aprobación de la DIRECTIVA REGIONAL N° 04-2022-G.R.PUNO "LINEAMIENTOS PARA EL USO DE FIRMAS Y CERTIFICADOS DIGITALES EN EL GOBIERNO REGIONAL PUNO";

CONSIDERANDO:

Que, por Ley N° 27269, se regula la utilización de la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad. Entiéndase por firma electrónica a cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención precisa de vincularse o autenticar un documento cumpliendo todas o algunas de las funciones características de una firma manuscrita;

Que, la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial del Gobierno Regional de Puno, en base a la norma precedente, ha formulado la Directiva Regional "Lineamientos para el uso de firmas y certificados digitales en el Gobierno Regional de Puno";

Que, la Directiva tiene por objeto regular y uniformizar el uso de las firmas digitales, otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita, producto de un acto administrativo que requiere ser firmado digitalmente;

Que, la Directiva Regional es de aplicación y cumplimiento obligatorio por los funcionarios y servidores públicos de las diferentes unidades de organización del Gobierno Regional de Puno, en el marco de sus funciones asignadas en los instrumentos de gestión institucional;

Que, es atribución del Gobernador Regional aprobar las normas reglamentarias de organización y funciones de las dependencias administrativas del Gobierno Regional en virtud del artículo 21, acápite h de la Ley Orgánica de Gobiernos Regionales, Ley N° 27867; y

Estando a la Opinión Legal N° 250-2022-GR PUNO/ORAJ de la Oficina Regional de Asesoría Jurídica;

En el marco de las funciones y atribuciones conferidas por la Constitución Política del Perú, Ley N° 27783, Ley N° 27867 y su modificatoria Ley N° 27902;

GOBIERNO REGIONAL PUNO

Resolución Ejecutiva Regional

Nº 342 -2022-GR-GR PUNO

PUNO, 18 JUL 2022

SE RESUELVE:

ARTICULO PRIMERO.- APROBAR la DIRECTIVA REGIONAL N° 04-2022-G.R.PUNO "LINEAMIENTOS PARA EL USO DE FIRMAS Y CERTIFICADOS DIGITALES EN EL GOBIERNO REGIONAL PUNO", que consta de diez (10) capítulos, Anexos: 01 y 02; y que en nueve (09) folios forma parte de la presente resolución.

ARTÍCULO SEGUNDO.- ENCARGAR el cumplimiento de la presente Directiva Regional a la Oficina Regional de Administración en coordinación con los demás órganos competentes.

REGÍSTRESE, COMUNÍQUESE Y ARCHÍVESE

GERMAN ALEJO APAZA
GOBERNADOR REGIONAL

GOBIERNO REGIONAL PUNO

DIRECTIVA REGIONAL N° 04 -2022-G.R. PUNO

LINEAMIENTOS PARA EL USO DE FIRMAS Y CERTIFICADOS DIGITALES EN EL GOBIERNO REGIONAL PUNO

I. FINALIDAD

Establecer lineamientos para el uso correcto de firmas y certificados digitales en la generación de documentos electrónicos, a fin de contribuir al proceso de transformación digital, eficacia de la gestión pública regional en las unidades de organización del Gobierno Regional Puno.

II. OBJETIVO

Regular y uniformizar el uso de las firmas digitales, otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita, producto de un acto administrativo que requiere ser firmado digitalmente.

III. BASE LEGAL

- Ley 27269, Ley de Firmas y Certificados Digitales, modificado por Ley 27310.
- Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado y su modificatoria.
- Ley N° 27867, Ley Orgánica de Gobiernos Regionales y sus modificatorias.
- Ley N° 29733, Ley de Protección de Datos Personales y su reglamento.
- Ley N° 31170, Ley que Dispone la Implementación de Mesas de Partes Digitales y Notificaciones Electrónicas.
- Decreto Legislativo Nº 1412, que aprueba la Ley de Gobierno Digital y su reglamento.
- Decreto de Urgencia N° 006-2020, que crea el Sistema Nacional de Transformación Digital.
- Decreto de Urgencia N° 007-2020, que aprueba el Marco de Confianza Digital y Dispone Medidas para su Fortalecimiento.
- Decreto Supremo 052-2008-PCM, que aprueba el Reglamento de la Ley de Firmas y Certificados Digitales, y su modificatoria por Decreto Supremo 070-2011-PCM.
- Decreto Supremo N° 050-2018-PCM, que aprueba la definición de Seguridad Digital en el Ámbito Nacional.
- Decreto Supremo Nº 044-2020-PCM, que declara en Estado de Emergencia Nacional por las graves circunstancias que afectan la vida de la Nación a consecuencia del brote del COVID-19 y sus modificatorias.
- Reglamento de Organización y Funciones del Gobierno Regional Puno, aprobado con Ordenanza Regional Nº 002-2018-GR PUNO CRP.

IV. ALCANCE

La presente directiva es de aplicación y cumplimiento obligatorio por los funcionarios/as y servidores/as públicos de las diferentes unidades de organización del Gobierno Regional Puno, en el marco de sus funciones asignadas en los instrumentos de gestión institucional.

V. DEFINICIONES

a. **Administrador del certificado digital.**- Es aquel servidor/a público acreditado por el titular de la unidad organizacional (unidades ejecutoras o unidades operativas, entre otros) del Gobierno Regional Puno, responsable de coordinar y gestionar los certificados digitales ante el Registro Nacional de Identificación y Estado Civil (RENIEC).

b. **Certificado digital.-** Es el documento electrónico usado como credencial, que ha sido generado y firmado digitalmente por una Entidad de certificación y que permite identificar a la persona natural o jurídica que emitirá la firma digital.

c. **Clave privada (PIN).-** Es una de las claves de un sistema de criptografía asimétrica que se emplea para generar una firma digital sobre un documento electrónico y es mantenida en reserva por el suscriptor o titular de la firma digital.

d. **Clave pública.-** Es la otra clave en un sistema de criptografía asimétrica que es usada por el destinatario de un documento electrónico para verificar la firma digital puesta en dicho documento. La clave pública puede ser conocida por cualquier persona.

e. **Documento electrónico.-** Es la unidad básica estructurada de información registrada, publicada o no, susceptible de ser generada, clasificada, gestionada, transmitida, procesada o conservada por una persona o una organización de acuerdo a sus requisitos funcionales, utilizando sistemas informáticos.

f. **Firma digital.-** Es aquella firma electrónica que utilizando una técnica de criptografía asimétrica, permite la identificación del signatario y ha sido creada por medios, incluso a distancia, que garantizan que éste mantiene bajo su control con un elevado grado de confianza, de manera que está vinculada únicamente al signatario y a los datos a los que refiere, lo que permite garantizar la integridad del contenido y detectar cualquier modificación ulterior, tiene la misma validez y eficacia jurídica que el uso de una firma manuscrita.

g. **Infraestructura Oficial de Firma Electrónica (IOFE).-** Sistema confiable, acreditado, regulado y supervisado por la autoridad administrativa competente, provisto de instrumentos legales y técnicos que permiten generar firmas digitales y proporcionar diversos niveles de seguridad respecto de: la integridad de los documentos electrónicos; y la identidad de su autor, lo que es regulado por Ley.

h. **Plataforma Integrada de la Entidad de Registro (PIER).-** Permite gestionar las solicitudes de emisión y cancelación de certificados digitales de persona jurídica y de agente automatizado de las entidades públicas del Estado Peruano.

i. **ReFirma PDF.-** Aplicativo informático que permite firmar digitalmente documentos en formato PDF, realizando las validaciones requeridas para la generación de firmas digitales con valor legal y con la misma eficacia jurídica que las firmas manuscritas, dentro del marco de la Infraestructura Oficial de Firma Electrónica (IOFE).

j. **Suscriptor de firma digital.-** Los suscriptores son las personas naturales responsables de la generación y uso de la clave privada, con excepción de los certificados digitales para su utilización a través de agentes automatizados, situación en la cual las personas jurídicas asumen las facultades de titulares y suscriptores del certificado digital.

k. **Titular de la firma digital.-** El titular de la firma digital es la persona a la que se le atribuye de manera exclusiva un certificado digital que contiene una firma digital, identificándolo objetivamente en relación con el mensaje de datos.

l. **Token.-** Es un dispositivo de almacenamiento criptográfico que contiene el Certificado Digital asignado a la persona titular del mismo, que le permite firmar digitalmente. El token u otro dispositivo de almacenamiento de certificado digital cumplen con el estándar FIPS 140-2, según convenio suscrito con el Registro Nacional de Identificación y Estadio Civil (RENIEC).

VI. RESPONSABILIDAD

6.1. La implementación y el cumplimiento de la presente directiva está a cargo de la Oficina de Tecnologías de Información y Comunicación o la que haga sus veces, Oficina de Recursos Humanos o quien haga sus veces y el Administrador o representante de la Entidad en las unidades de organización del Gobierno Regional Puno.

6.2. Los representantes de las unidades de organización (unidades ejecutoras o unidades operativas, entre otros), son servidores/as públicos acreditados mediante acto administrativo, son responsables de tramitar los certificados digitales ante el Registro Nacional de Identificación y Estado Civil (RENIEC).

6.3. Son responsables los funcionarios/as y servidores/as públicos autorizados, son responsables de la generación de su clave privada y del uso de la firma digital.

6.4. La Oficina de Recursos Humanos o la que haga sus veces en las unidades de organización,son responsables de autorizar y/o reportar cancelación del certificado digital en caso de cese de sus funciones.

6.5. La Oficina de Tecnologías de Información y Comunicación o quien haga sus veces y el Administrador o Representante de la Entidad, es el responsable de capacitar a los funcionarios/as y servidores/as públicos e instalar el certificado digital y el aplicativo informático, para el uso adecuado de las firmas digitales.

6.6. La Oficina Regional de Administración o quien haga sus veces, es responsable de asumir el costo del trámite de los certificados digitales por primera vez ante el Registro Nacional de Identificación y Estado Civil (RENIEC).

6.7. La responsabilidad sobre los efectos jurídicos generados por la utilización de la firma digital corresponde al suscriptor o titular de la firma.

VII. DISPOSICIONES GENERALES

Los funcionarios/as y servidores/as públicos del Gobierno Regional Puno, son responsables de aplicar la presente directiva en la generación de documentos electrónicos, en los diferentes trámites administrativos que requieran ser firmados digitalmente.

7.1. De las firmas y certificados digitales

La suscripción de un documento electrónico con firma digital generado desde un certificado digital vigente, es un mecanismo tecnológico que posee validez y eficacia jurídica.

A la firma electrónica se le aplica un software digital acreditado ante la autoridad administrativa competente, convirtiéndose en una firma digital, que tendrá los siguientes beneficios:

- Simplificación administrativa
- Aportar el aumento de la confianza digital
- Aportar al desarrollo del gobierno y transformación digital
- Otorgar mayor seguridad e integridad a los documentos

7.2. De la validez

a. La firma digital generada tiene la misma validez y eficacia jurídica que el uso de una firma manuscrita.

b. Los documentos electrónicos firmados digitalmente pueden ser admitidos como prueba en los procesos judiciales y/o procedimientos administrativos.

c. La comprobación de la validez de un documento firmado digitalmente se realiza en un ambiente electrónico aplicando el software de verificación de la firma digital, ReFirma PDF o algún otro acreditado por la autoridad competente.

d. La vigencia del certificado digital, es de un año a partir de su fecha de emisión y esta puede ser renovada a solicitud del suscriptor de la firma.

7.3. De la invalidez.- Una firma digital carece de validez, cuando:

a. Es utilizada en fines distintos para los que fue extendido el certificado, su uso es exclusivo para el cumplimiento de las funciones de los funcionarios/as y servidores/as públicos.

b. El certificado haya sido cancelado conforme a lo establecido en el Decreto Supremo 052-2008-PCM, reglamento de la Ley de Firmas y Certificados Digitales y sus modificatorias.

7.4. Del Administrador del Certificado Digital.- Es un servidor público acreditado por el titular de la unidad organizacional, quién es responsable de coordinar y gestionar los Certificados Digitales ante el Registro Nacional de Identificación y Estado Civil (RENIEC) a través de un formulario llamado solicitud de acceso al servicio de emisión de certificados digitales, el mismo que tiene que ser informado ante el Registro Nacional de Identificación y Estado Civil (RENIEC). Para dicho efecto, el Administrador del Certificado Digital debe seguir los pasos o procedimientos establecidos en la Plataforma Integrada de Entidad de Registro (PIER).

VIII. DISPOSICIONES ESPECÍFICAS

8.1. De la solicitud del certificado digital

8.1.1. La Oficina de Recursos Humanos o quien haga sus veces de las unidades de organización (unidades ejecutoras, unidades operativas, y otros), es la responsable de manera obligatoria implementar el certificado de firma digital para cada servidor público.

8.1.2. Para la autorización del certificado digital, el funcionario/a o servidor/a público debe solicitar a la Oficina de Recursos Humanos o a quien haga sus veces adjuntando la documentación siguiente:

a. Declaración Jurada de identificación no presencial para solicitar certificado digital persona jurídica en el marco de los D.S N°008-2020-SA y D.S N° 044-2020-PCM que declara el Estado de Emergencia Nacional.

b. Copia de DNI vigente.

c. Copia del documento que acredite el vínculo laboral y el cargo que ocupa en la Entidad.

d. Comprobante de pago por concepto de emisión de certificados digitales para entidades de la administración pública ante el Registro Nacional de Identificación y Estado Civil (RENIEC).

8.1.3. La Oficina Recursos Humanos o la que haga sus veces en las unidades de organización, dispone el requerimiento del certificado digital del suscriptor al Representante o Administrador de Certificados Digitales, verificación de los requisitos y/o cancelación del certificado digital, para su trámite correspondiente ante el Registro Nacional de Identificación y Estado Civil (RENIEC).

8.1.4. Es obligación del suscriptor entregar información veraz durante la solicitud de emisión de certificados y demás procesos de certificación (cancelación, suspensión, reemisión y modificación).

8.2. De la emisión, renovación y reemisión del certificado digital.

8.2.1. De la emisión

a. El suscriptor (funcionario/a o servidor/a público autorizado) recibirá por correo electrónico una clave y la ruta de descarga del Certificado Digital emitido por el Registro Nacional de Identificación y Estado Civil (RENIEC).

b. El suscriptor es responsable de revisar su correo electrónico, en la bandeja de entrada o en la bandeja de correo no deseado, la emisión de dicho certificado y sus instrucciones por el Registro Nacional de Identificación y Estado Civil (RENIEC).

c. Una vez recibido el correo electrónico del Registro Nacional de Identificación y Estado Civil (RENIEC), el suscriptor/a debe comunicase con el Administrador del Certificado Digital, para la implementación del certificado digital en el equipo de cómputo, laptop o Token a su cargo (homologado por RENIEC) según corresponda.

d. El Administrador de Certificados Digitales o la Oficina de Recursos Humanos o quien haga sus veces, no se responsabiliza de la expiración de los certificados digitales.

8.2.2. De la renovación y reemisión

a. El suscriptor solicita la renovación de su certificado digital al Administrador de Certificados Digitales, antes del plazo de su expiración.

b. El suscriptor solicita la reemisión de su certificado digital al Administrador de Certificados Digitales, por perdida de contraseña, mala instalación, vencimiento de plazo de descarga, extravió de equipo de cómputo o formateo de ordenador que no es propiedad de la Entidad, entre otros. Para su trámite, el suscriptor asume el costo, no requiere declaración jurada y no procede solicitar la reemisión de un certificado digital caducado.

c. La reemisión de certificado digital por daño físico o lógico del ordenador, así como, la renovación antes del plazo de expiración y otros de la Entidad, el pago será asumida por la misma unidad organizacional.

8.3. De la instalación de la firma digital

a. El Administrador del Certificado Digital, en coordinación con el suscriptor autorizado ejecuta la instalación del certificado digital, para ello el interesado debe brindar la información proporcionada por parte del Registro Nacional de Identificación y Estado Civil (RENIEC) bajo responsabilidad.

b. El suscriptor que realiza trabajo remoto o presencial debe disponer como mínimo de un computador (PC) u ordenador con acceso a internet, sistema operativo Windows 7 de 32 o 64 bits o superior.

c. En el proceso de instalación del certificado digital en un ordenador, el Administrador del Certificado Digital, solicita al suscriptor ingrese o cree una contraseña (PIN) confidencial, la cual servirá, para que pueda firmar a partir de ese momento los documentos electrónicos.

d. Una vez instalado el certificado digital, el suscriptor debe firmar una conformidad de la conclusión de la instalación, configuración y capacitación. Anexo N° 02.

8.4. Del uso de la firma digital

a. El Administrador del Certificados Digitales, es responsable de asegurar la usabilidad, de coordinar y gestionar la emisión de los certificados digitales.

b. El certificado de firma digital es personal e intransferible, por lo que solo el suscriptor del mismo debe tener acceso a él.

c. No revelar o anotar la clave privada (PIN) en algún lugar, por su seguridad.

d. El suscriptor por seguridad, no debe permitir a otra persona firme por él.

e. Contar con una guía para el uso adecuado del software de firma digital.

f. Leer el contenido íntegro del documento, previa a la firma digital.

g. Al generar y firmar un documento, no olvide enviarlo en forma digital al destinatario.

h. El suscriptor al recibir un documento firmado digitalmente, debe verificar su autenticidad y veracidad.

i. Asegurarse de un buen equipo de cómputo, sistema antivirus y mantener actualizado. No debe instalar software de fuentes desconocidas, ni navegar por sitios que inspiren poca confianza.

j. El suscriptor debe informar al Administrador del Certificado Digital, en caso de pérdida y robo del ordenador o dispositivo electrónico.

k. Custodiar todo documento electrónico firmado digitalmente hasta la entrega del cargo, bajo responsabilidad.

8.5. De la solicitud de cancelación del certificado digital

El Administrador del Certificado Digital, realizará la gestión de la cancelación de los certificados digitales ante el Registro Nacional de Identificación y Estado Civil (RENIEC) por las causales siguientes:

a. A solicitud del suscriptor y/o el titular del certificado digital, siendo necesario para tal efecto la aceptación del Registro Nacional de Identificación y Estado Civil (RENIEC).

b. Por decisión de la Entidad de certificación.

c. Por expiración del plazo de vigencia.

d. Por resolución administrativa o judicial que ordene la cancelación del certificado.

e. Por interdicción civil judicialmente declarada o declaración de ausencia o de muerte presunta, del titular del certificado.

f. Por muerte, o por inhabilitación o incapacidad declarada judicialmente de la persona natural suscriptor del certificado.

g. Por solicitud de un tercero que informe y pruebe de manera fehaciente alguno de los supuestos de revocación contenidos en el artículo 10 de la Ley N° 27269.

h. Por cese de funciones.

i. Otras causales que establezca la autoridad administrativa competente.

IX. DISPOSICIONES COMPLEMENTARIAS

Los supuestos no previstos en la presente Directiva, se encuentran reguladas en la Ley N° 27269, Ley de Firmas y Certificados Digitales; modificatoria y su reglamento; así como, las disposiciones emitidas por el Registro Nacional de Identificación y Estado Civil (RENIEC) y por la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros.

X. ANEXO

Anexo N° 01: Declaración Jurada de identificación no presencial para solicitar certificado digital persona jurídica en el marco de los D.S N°008-2020-SA y D.S N° 044-2020-PCM que declara el estado de emergencia nacional.

Anexo N° 02: Conformidad de Instalación de Certificado Digital.

GOBIERNO REGIONAL PUNO V°B° Gerencia Regional de Planeamiento, Presupuesto y A.T. PUNO

Puno, mayo del 2022

GOBIERNO REGIONAL PUNO VISACIÓN Sub Gerente de M. D.I.

GOBIERNO REGIONAL PUNO

ANEXO N° 01

DECLARACIÓN JURADA DE IDENTIFICACIÓN NO PRESENCIAL PARA SOLICITAR CERTIFICADO DIGITAL PERSONA JURÍDICA EN EL MARCO DE LOS D.S N°008-2020-SA Y D.S N° 044-2020-PCM QUE DECLARA EL ESTADO DE EMERGENCIA NACIONAL

El Suscrito,

_____

Identificado (a) con DNI N° _____, de fecha de emisión ____/____/____ (verificar el dato en su documento físico).

Información del trabajador (En departamento, provincia y distrito consignar de acuerdo a su sede laboral)

Entidad: **GOBIERNO REGIONAL PUNO**

Departamento: Provincia: Distrito:

Correo electrónico: _____

DECLARO ante RENIEC, que la información consignada es veraz, y se remite a fin de iniciar el trámite de mi Certificado Digital de Persona Jurídica para uso institucional.

Para dar conformidad, adjunto como evidencia mi fotografía y firma, a fin de que sea evaluada como sustento en la aprobación de mi trámite para la obtención de mi certificado digital.

FOTOGRAFIA ACTUAL SIN GAFAS del titular diferente al DNI ADEMAS, SI LA SOLICITUD ES VIRTUAL: La fotografía puede ser un selfie con el celular (autofoto) No escanear foto	(FIRMA DEL TITULAR DENTRO DEL RECUADRO) SI LA SOLICITUD ES VIRTUAL: Firmar la presente para luego escanearlo.

IMPORTANTE; La firma debe ser la misma consignada en el DNI, caso contrario el trámite será denegado.

Lugar y fecha: _____

En caso de falsa declaración en procedimiento administrativo se aplicará el Artículo 411 del Cód. Penal: "El que, en un procedimiento administrativo, hace una falsa declaración en relación a hechos o circunstancias que le corresponde probar, violando la presunción de veracidad establecida por ley, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años".

(*) Esta declaración jurada no debe tener una antigüedad mayor a 30 días

GOBIERNO REGIONAL PUNO

ANEXO N° 02

CONFORMIDAD DE INSTALACIÓN DE CERTIFICADO DIGITAL

El que suscribe: _____Funcionario y/o trabajador del Gobierno Regional Puno, identificado con DNI: _____del(la):_____con el Cargo de: _____ manifiesta que el CERTIFICADO DIGITAL, solicitado ha sido instalado satisfactoriamente en:

- PC ☐
- LAPTOP ☐
- Token ☐

Además, he recibido la capacitación básica en el uso del mismo para firmar digitalmente, en fecha: _____/_____/_____. También, es necesario señalar que este Certificado Digital solo será utilizado con fines que involucren sus funciones en el Gobierno Regional Puno.

_____

Firma y sello del suscrito

GOBIERNO REGIONAL PUNO VISACIÓN Sub Gerente de M y D.I.