Resolución de Gerencia General

N° 028-2024-UESST/GG

Tumbes, 17 de julio de 2024

VISTO: El Informe N° 117-2024-UESST-GAF-OTI de la Oficina de Tecnología de la Información; el Informe N° 326-2024-UESST-GAF; y,

CONSIDERANDO:

Que, el Organismo Técnico de la Administración de los Servicios de Saneamiento, como organismo público técnico especializado adscrito al Ministerio de Vivienda, Construcción y Saneamiento, en marco de la Resolución Ministerial N° 374-2018-VIVIENDA, formaliza a través de la Resolución Directoral N° 095-2018-OTASS-DE, la creación de la Unidad Ejecutora 002 Servicios de Saneamiento Tumbes en el Pliego 207: Organismo Técnico de la Administración de los Servicios de Saneamiento, encargado a partir del 01 de diciembre de 2018, prestar los servicios de saneamiento en el ámbito de Tumbes, Zarumilla y Contralmirante villar;

Que, de acuerdo al Manual de Gestión Operativa de la Unidad Ejecutora 002 Servicio de Saneamiento Tumbes, aprobado por Resolución de Consejo Directivo N° 009-2018-OTASS/CD, el gerente general es el máximo órgano de gestión administrativa, de la referida unidad ejecutora, responsable de ejecutar las decisiones acordadas por la Dirección Ejecutiva del OTASS;

Que, el artículo 29 de la Resolución Directoral N° 009-2018-OTASS/CD, preceptúa que la Oficina de Tecnología de la Información, es la unidad orgánica que depende de la Gerencia de Administracion y Finanzas, responsable de desarrollar, implementar y gestionar sistemas de inbformacion, bases de datos, infraestructura tecnologica y telecomunicaciones, establecer los mecanismos que aseguren la integridad y confidencialidad de la informacion digitalizada, asi como del soporte y mantenimiento para la operatividad de las redes, equipos informaticos y el buen uso del software y hardware de la UESST;

Que, a través del Informe N° 326-2024-UESST-GAF, la Gerencia de Administración y Finanzas de la Unidad Ejecutora 002 Servicios de Saneamiento Tumbes, sobre la base del Informe N° 117-2024-UESST-GAF-OTI, de la Oficina de Tecnología de la Información -en calidad de área usuaria-, solicita a Gerencia General la aprobación de la directiva que establece los "Lineamientos para la uniformidad en el uso de los certificados y firmas digitales de los trabajadores de la Unidad Ejecutora 002 Servicios de Saneamiento Tumbes";

Que, en ese sentido y estando a lo informado por los documentos de Vistos, resulta necesario expedir el acto resolutivo que aprueba la directiva que establece los "Lineamientos para la uniformidad en el uso de los certificados y firmas digitales de los trabajadores de la Unidad Ejecutora 002 Servicios de Saneamiento Tumbes";

Resolución de Gerencia General

Con el visado de la Gerencia de Administración y Finanzas y de la Oficina de Asesoría Jurídica;

De conformidad con lo dispuesto en la Resolución Ministerial N° 374-2018-VIVIENDA, que declara la caducidad del contrato de concesión, la Resolución Directoral N° 095-2018-OTASS-DE, que crea la Unidad Ejecutora 002: denominada Servicios de Saneamiento Tumbes y la Resolución de Consejo Directivo N° 009-2018-OTASS/CD;

SE RESUELVE:

Artículo 1.- Aprobar la Directiva N° 002-2024-UESST/GG, directiva que establece los "Lineamientos para la uniformidad en el uso de los certificados y firmas digitales de los trabajadores de la Unidad Ejecutora 002 Servicios de Saneamiento Tumbes", que en anexo adjunto forma parte integrante de la presente resolución.

Artículo 2.- La Gerencia de Administración y Finanzas, a través de la Oficina de Tecnología de la Información, serán responsable de cumplir con lo dispuesto en el artículo 1 de la presente resolución, en el marco de sus competencias, para lo cual deberán ser comunicados con el contenido de la presente resolución.

Artículo 3.- Disponer la publicación de la presente resolución y el anexo en el Portal Institucional: www.aguatumbes.gob.pe.

DISPOSICIONES COMPLEMENTARIAS

Primera.- Los documentos electrónicos firmados digitalmente se almacenan en el sistema de trámite documentario de Agua Tumbes o el almacén digital que haga sus veces.

Segunda.- La clave privada es almacenada de manera segura en un dispositivo criptográfico que cumpla con el *Estándar FIPS 140-2 sección 4.7.2 o Common Criteria EAL4+*, y está en posesión del suscriptor del certificado digital (tarjeta inteligente, token o disco duro de la computadora).

Tercera.- Considerando que la firma digital de un documento, implica la incorporación de código cifrado como parte de la estructura del archivo, solo es necesario insertar la firma por UNA SOLA VEZ al documento, con lo cual TODO el archivo se considera firmado y aceptado. Es decir, que con una única firma se cierra el documento y toda la información se cifra y acepta.

Regístrese, comuníquese y archívese.

NÍCIDA GISSELA PAREDES HASÉN
Gerente General
UE002 Servicios Saneamiento Tumbes

"LINEAMIENTOS PARA LA UNIFORMIDAD EN EL USO DE LOS CERTIFICADOS Y FIRMAS DIGITALES DE LOS TRABAJADORES DE LA UNIDAD EJECUTORA 002 SERVICIOS DE SANEAMIENTO TUMBES -AGUA TUMBES"

GERENCIA GENERAL Agua Tumbes V°B°

JEFE DE ADMINISTRACIÓN Agua Tumbes V°B°

JEFE DE OFICINA DE ASESORÍA JURÍDICA Agua Tumbes V°B°

2024

ÍNDICE

DIRECTIVA N° 002-2024-UESST/GG

I. FINALIDAD

Implementar el uso de la firma digital en los documentos que emiten los servidores de las diversas gerencias, unidades y oficinas de Agua Tumbes, con el fin de contribuir al Proyecto Cero Papel como parte de la política y aporte al gobierno electrónico.

II. OBJETIVO

Establecer los lineamientos para la uniformidad en el uso de los certificados y firmas digitales de los trabajadores de Agua Tumbes.

III. BASE NORMATIVA

3.1 Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado.
3.2 Ley N° 27269, Ley de Firmas y Certificados Digitales.
3.3 Decreto Legislativo N° 681: Regula el uso de tecnologías avanzadas en materia de archivo de documentos e información tanto respecto a la información elaborada en forma convencional y la producida por procedimientos informáticos en computadoras.
3.4 Decreto Legislativo N° 827: Amplían los alcances del D. Leg. 681 a las entidades públicas a fin de modernizar el sistema de archivos oficiales.
3.5 Decreto Legislativo N° 1310, Aprueba medidas adicionales de simplificación administrativa.
3.6 Decreto Supremo N° 001-2015-MINEDU, que aprueba el Reglamento de Organización y Funciones del Ministerio de Educación.
3.7 Decreto Supremo N° 081-2013-PCM, que aprueba la Política de Gobierno Electrónico 2013-2017.
3.8 Decreto Supremo N° 004-2013-PCM, que aprueba la Política Nacional de Modernización de la Gestión Pública.
3.9 Decreto Supremo N° 105-2012-PCM, que establece disposiciones para facilitar la puesta en marcha de la firma digital y modifica el Decreto Supremo N° 052-2008-PCM, Reglamento de la Ley de Firmas y Certificados Digitales.
3.10 Decreto Supremo N° 070-2011-PCM, que modifica el Reglamento de la Ley N° 27269, Ley de Firmas y Certificados y establece normas aplicables al procedimiento registral en virtud del Decreto Legislativo N° 681 y Ampliatorias.
3.11 Decreto Supremo N° 052-2008-PCM, que aprueba el Reglamento de la Ley N° 27269, Ley de Firmas y Certificados Digitales.
3.12 Decreto Supremo N° 004-2013-PCM, que aplica la Política Nacional de Modernización de la Gestión Pública al 2021.
3.13 Decreto Supremo N° 033-2018-PCM que crea la Plataforma Digital Única del Estado Peruano y establecen disposiciones adicionales para el desarrollo del Gobierno Digital.
3.14 Decreto Supremo N° 123-2018-PCM que aprueba el Reglamento del Sistema Administrativo de Modernización de la Gestión Pública.
3.15 Decreto Supremo N° 004-2019-JUS, Decreto Supremo que aprueba el Texto Único Ordenado de la Ley N° 27444 Ley del Procedimiento Administrativo General. Las normas señaladas incluyen sus respectivas modificatorias.
3.16 Decreto Supremo N° 005-2020-VIVIENDA, que aprueba el Texto Único Ordenado del Decreto Legislativo N° 1280, Ley Marco de la Gestión y Prestación de los Servicios de Saneamiento.
3.17 Decreto Legislativo N° 1620, Decreto Legislativo que modifica el Decreto Legislativo Nº 1280, Decreto Legislativo que aprueba la Ley Marco de la Gestión y Prestación de los Servicios de Saneamiento.

3.18 Resolución Ministerial N° 374-2018-VIVIENDA, que declara la caducidad del Contrato de Concesión para la mejora, ampliación, mantenimiento, operación y explotación de la infraestructura y los servicios de agua potable y alcantarillado sanitario en la jurisdicción de los municipios provinciales de Tumbes, Zarumilla y Contralmirante Villar y municipios distritales correspondientes.

3.19 Resolución Directoral N° 095-2018-OTASS/DE, formaliza la creación de la Unidad Ejecutora 002 Servicios de Saneamiento Tumbes, en el pliego 207: Organismo Técnico de la Administración de los Servicios de Saneamiento, cuyo nombre comercial será Agua Tumbes".

3.20 Resolución de Concejo Directivo N° 009-2018-OTASS/CD, aprueba el Manual de Gestión Operativa de la Unidad Ejecutora 002 Servicios de Saneamiento Tumbes.

IV. ALCANCE

Las disposiciones contenidas en la presente Directiva son de aplicación y cumplimiento obligatorio para todo el personal de las diversas gerencias, unidades y oficinas de Agua Tumbes, que cuentan con un certificado digital, y que en el ejercicio de sus funciones deban firmar digitalmente documentos electrónicos en el marco de los procesos de las unidades funcionales a las que pertenecen.

V. RESPONSABILIDAD

El jefe de la Oficina de Tecnología de la Información y el Administrador de Certificados Digitales son los responsables de velar por el fiel cumplimiento de las disposiciones contenidas en la presente directiva.

VI. DISPOSICIONES GENERALES

6.1 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.

La firma digital electrónica tiene la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve a manifestación de voluntad; y si a esta firma electrónica se le aplica un software de firma digital acreditado ante la autoridad administrativa competente, entonces la firma electrónica se convertirá en una firma digital que tendrá los siguientes beneficios:

a) Simplificación administrativa
b) Aportar el aumento de la confianza electrónica
c) Aportar el desarrollo del gobierno electrónico
d) Otorgar mayor seguridad e integridad a los documentos

6.2 Clave pública y privada

La firma digital se basa en la propiedad sobre un mensaje o documento cifrado (resumen hash) utilizando la clave privada de un suscriptor de certificado digital y ésta sólo puede ser descifrado utilizando la clave pública asociada. De tal manera, se tiene la seguridad que el mensaje o documento que ha podido descifrarse utilizando la clave pública sólo pudo cifrarse utilizando la clave privada.

VII. DISPOSICIONES ESPECÍFICAS

7.1 Emisión del Certificado Digital

7.1.1 El trámite de certificado digital se inicia con la manifestación de necesidad de la oficina de firmar digitalmente los documentos, lo cual se solicita mediante formato

de Solicitud de Firma Digital según Anexo N° 01, la que es alcanzada al Administrador de Certificados Digitales, junto a la constancia de pago de la tasa correspondiente según Anexo N° 02, para su trámite correspondiente.

7.1.2 La Gerencia General de Agua Tumbes, mediante resolución designa al Administrador del Certificado Digital, quién es el responsable de coordinar las gestiones de Certificados Digitales ante RENIEC.

7.1.3 La designación del Administrador del Certificado Digital es informada a EREP-RENIEC, por el gerente general de Agua Tumbes, a través de un formulario llamado Solicitud de Acceso al Servicio de Emisión de Certificados Digitales.

7.1.4 El Administrador del Certificado Digital debe seguir los pasos establecidos en la guía temporal para el representante de entidad: generación de lista de aspirantes a suscriptor, colgado dentro de la web del EREP- RENIEC en Manuales de la Plataforma Integrada de Entidad de Registro. ***https://pki.reniec.gob.pe/pier/***, siguientes

a) Registrar los datos de los suscriptores a través de la Plataforma Integrada de la Entidad de Registro – PIER del EREP-RENIEC.

b) Para crear la "Lista de Aspirantes a Suscriptor" se adjuntará por cada aspirante:

- Una declaración jurada que será completada por el suscriptor adjuntando su fotografía reciente (podría ser capturada con su celular) y firmada, la firma debe ser la consignada en su DNI, el cual servirá como sustento. (Según Anexo N° 1)

- Constancia de pago de la tasa 00529-Emisión De Certificados Digitales Para Entidades De La Administración Pública en el banco de la nación y/o por la web www.pagalo.pe. (Según Anexo N° 2)

c) La plantilla descargada contiene el formato de Declaración Jurada que deberán rellenar y firmar los aspirantes a suscriptor, la cual el Suscriptor con el rol de representante de entidad deberá firmar digitalmente (en formato PDF) por cada registro del listado de aspirantes a suscriptor que desea generar.

d) El suscriptor recibirá por correo electrónico una clave y la ruta para descargar el Certificado Digital emitido por la EREP-RENIEC en un plazo máximo de cinco (05) días hábiles en el correo electrónico consignado, en caso de no consignar correo electrónico se utilizará por defecto el correo de la jefatura de la Oficina de Tecnología de la Información. El suscriptor será responsable de revisar su correo tanto en la bandeja de entrada como en la bandeja de correo no deseado, la emisión de dicho certificado y sus instrucciones correspondiente por la EREP-RENIEC salvo se haya utilizado el correo por defecto en cuyo caso la responsabilidad de seguimiento recaerá en esa oficina.

e) Una vez recibido el correo electrónico del EREP-RENIEC, el suscriptor deberá comunicarse con la Oficina de Tecnología de la Información, para que procedan a la instalación del certificado digital en su equipo de cómputo. En el proceso de instalación del Certificado Digital se solicitará que el suscriptor ingrese una contraseña, la cual servirá, para que pueda firmar a partir de ese momento los documentos electrónicos.

En caso que la unidad orgánica considere conveniente, determinará quién o quiénes podrán hacer uso de la instalación del certificado digital mediante un token u otro dispositivo de almacenamiento del certificado digital. Se solicitará

que el suscriptor ingrese un Pin, el cual servirá, para que pueda firmar a partir de ese momento los documentos electrónicos.

7.2 Del uso del certificado digital para la firma digital de los suscriptores

7.2.1 Los gerentes y jefes de las diversas unidades orgánicas, deberán de velar por el correcto uso de la firma digital en sus áreas de trabajo funcionales.

7.2.2 Para que un suscriptor pueda utilizar la firma digital en los documentos electrónicos, debe contar con el Certificado Digital, un dispositivo electrónico de seguridad que almacena su clave privada (token criptográfico y/o computador) y el Software de Firma Digital.

7.2.3 Los suscriptores harán uso de los certificados digitales para firmar digitalmente documentos electrónicos de acuerdo a las funciones y procedimientos de su competencia. El uso de la contraseña de su certificado digital es intransferible, siendo responsabilidad del suscriptor el uso de la firma de cualquier documento electrónico usando su usuario contraseña, lo que generará el *no repudio* de esta ni siquiera por el propio suscriptor dueño de la firma y certificado digital.

7.2.4 Con relación al uso de la clave privada y del certificado digital por parte del suscriptor, este deberá cumplir con lo siguiente:

a) Emplear adecuadamente su certificado digital conforme a lo dispuesto en la Ley N° 27269 – Ley de Firmas y Certificados Digitales y su Reglamento y sus modificatorias

b) Mantener el control y absoluta reserva de la clave privada bajo su responsabilidad y debe ser conocida únicamente por él.

c) En caso de extravío o pérdida de la tarjeta inteligente o token criptográfico se estaría garantizando que; nadie que no conozca dicha contraseña o PIN de acceso, pueda hacer uso de su firma digital

d) Custodiar su contraseña o PIN de acceso de forma diligente, tomando las precauciones razonables para evitar su pérdida, revelación, modificación o uso no autorizado.

e) En caso de que la clave privada quede comprometida en su seguridad, el suscriptor debe notificarlo de inmediato al Administrador del Certificado Digital; para que proceda a la cancelación del certificado digital.

7.2.5 Los suscriptores son responsables del contenido de los documentos electrónicos firmados digitalmente.

7.2.6 El suscriptor debe elaborar el documento y convertirlo a formato PDF para firmarlo digitalmente. En caso no se haya efectuado la firma digital, podrá modificar el documento las veces que sea necesario para su posterior firma.

7.2.7 Para firmar digitalmente un documento electrónico, se deberá seleccionar y cargar el documento electrónico a firmar mediante el Software de Firma

En caso se requiere firmar documentos de forma masiva se deberá realizar la firma en bloque.

7.2.8 En caso el suscriptor deba firmar un documento electrónico firmado previamente por otro trabajador, deberá verificar la validez de la firma y que el documento no haya sufrido modificaciones.

7.3 Del procedimiento de cancelación y anulación de la solicitud de los certificados digitales

7.3.1 Procede en los siguientes casos:

a) Cuando por error de la Oficina solicitante y/o del Administrador del Certificado Digital se haya consignado información inexacta en la solicitud.

b) Por deterioro, alteración o cualquier otro hecho que afecte la clave privada o la contraseña de acceso a su clave privada.

c) Por la pérdida, robo o extravío del dispositivo electrónico de seguridad que almacena su clave privada (computador o token criptográfico).

d) Cada vez que haya desvinculación o rotación de personal el Jefe de la unidad orgánica a la que se encuentre asignado el personal remitirá al Administrador del Certificado Digital la relación de personal con su DNI.

e) Cuando el suscriptor del certificado digital solicite mediatamente al Administrador del Certificado Digital la cancelación de su certificado, ello, cuando sospeche el compromiso potencial de su clave privada, debido a la pérdida de su contraseña o sospecha que un tercero conozca o pueda deducir dicha contraseña.

7.3.2 El Administrador del Certificado Digital deberá seguir los pasos establecidos en la guía de usuario: operador de registro digital, colgado dentro de la web del EREP-RENIEC en Manuales de la Plataforma Integrada de Entidad de Registro, sección del Manual: Cancelación de Certificados Digitales. https://pki.reniec.gob.pe/pier/

7.4 La administración del Token Criptográfico

7.4.1 El administrador del Certificado Digital, asignará un token a cada suscriptor en caso sean justificadamente requeridos y se cuente con stock.

7.4.2 En el caso de solicitud de token para otras posiciones que no sean funcionario, el responsable de la oficina remitirá al Administrador del Certificado Digital, la relación de servidores que visarán y/o firmarán los documentos, debiendo llenar el Formato de Requerimiento de Dispositivo Criptográfico – Token.

7.4.3 La asignación del token la realiza el Administrador del Certificado Digital, se efectúa mediante el formato de Asignación de Dispositivo Criptográfico.

7.4.4 El Administrador de Certificado Digital, instruye a los suscriptores, respecto al almacenamiento del certificado en el token.

7.4.5 En caso de bloqueo de password o PIN del token, el suscriptor está en la obligación de comunicar al Administrador del Certificado Digital, quién verifica si se trata de un bloqueo momentáneo o permanente. Si fuera un bloqueo permanente, el Administrador del Certificado Digital, se comunica con la EREP- RENIEC para la revocación del certificado digital y generación de uno nuevo.

7.4.6 El suscriptor es responsable del token criptográfico asignado. En caso este haya sido perdido, sustraído, deteriorado, averiado o robado, éste deberá ser sustituido con otro token con características iguales o mejores, el cual debe ser aprobado.

7.4.7 En el caso de cese de labores, el suscriptor deberá devolver el Dispositivo Electrónico como parte de la entrega de cargo al Administrador del Certificado Digital.

VIII. RESPONSABILIDADES DE LOS INTERVINIENTES EN EL CERTIFICADO DIGITAL

8.1 El Administrador del Certificado Digital

a) Entregar información veraz durante la solicitud de emisión de certificados y demás procesos: suspensión, anulación, cancelación ante RENIEC.

b) Cumplir permanentemente las condiciones establecidas por la Entidad de Certificación para la utilización del Certificado.

c) Solicitar la generación, renovación, actualización, cancelación o anulación de los certificados digitales ante la EREP-RENIEC.

d) El Administrador del Certificado Digital solicita a la EREP-RENIEC la emisión y cancelación de los certificados digitales del/ la suscriptor/a, asumiendo las obligaciones del Titular, estipuladas en el artículo 15 del Reglamento de la Ley de Firmas y Certificados Digitales, aprobado con Decreto Supremo N° 052-2008-PCM.

8.2 La Oficina de Tecnologías de la Información

a) Brindar capacitación y asistencia técnica en el uso del dispositivo de almacenamiento de certificado digital o token.

b) Atender las incidencias técnicas de los suscriptores con respecto a la instalación de los certificados digitales y uso de las firmas digitales bajo las plataformas de generación y trazabilidad de los documentos INTRANET, así como por otras plataformas de Firma Digital como el REFIRMA, PERUFIRMA u otros.

c) Incorporar las medidas técnicas orientadas a mantener la integridad del documento electrónico con firma digital y que la información que contenga sea accesible para su posterior consulta.

8.3 El Suscriptor

a) Todo suscriptor que tiene asignado un token u otro dispositivo de almacenamiento de certificado digital es responsable de cambiar el PIN para su uso. Puede realizar los cambios de PIN que considere convenientes a través de la opción de gestión de dispositivo, pudiendo solicitar el apoyo de la Oficina de Tecnología de la Información, siendo responsable de mantener la confidencialidad de la misma.

b) Emplear adecuadamente su certificado digital, conforme a la normativa vigente.

c) Dejar de utilizar la clave privada, transcurrido el plazo de vigencia del certificado digital.

d) Notificará a la EREP- RENIEC, a través del Administrador de los Certificados Digitales sin retrasos las inexactitudes o cambios en el contenido del certificado digital.

e) Proteger el acceso al repositorio del certificado digital (computador, tarjeta inteligente, token criptográfico).

f) Verificar la validez de las firmas digitales existentes en el Documento PDF, de acuerdo al procedimiento descrito en el **Anexo N° 3: Verificación de la firma digital.**

IX. DE LAS SANCIONES

9.1 En caso de incumplimiento de las disposiciones establecidas en la presente directiva, deberá aplicarse una sanción de acuerdo con la gravedad de las actuaciones e infracciones.

9.2 El proceso para la determinación y aplicación de la sanción se desarrollará de acuerdo con las fases del Procedimiento Administrativo Disciplinario (PAD), en estricto cumplimiento a lo establecido en el Reglamento Interno de Trabajo establecido en Agua Tumbes.

9.3 Las autoridades y la sanción a imponer en el Procedimiento Administrativo Disciplinario (PAD), serán definidas de acuerdo con el tipo de sanción a imponer.

Para efectos de identificar al Órgano Instructor y Sancionador se adjunta el siguiente detalle:

SANCIÓN	ÓRGANO INSTRUCTOR	ÓRGANO SANCIONADOR	OFICIALIZACIÓN DE LA SANCIÓN
Amonestación escrita	Jefe inmediato		Oficina de Recursos Humanos
Suspensión	Jefe Inmediato	Jefe de Recursos Humanos	Oficina de Recursos Humanos
Despido	Jefe/a de Unidad de Recursos Humanos	Gerencia General	Gerencia General

Durante el desarrollo del Procedimiento Administrativo Disciplinario (PAD), el órgano instructor y órgano sancionador, contarán con el apoyo y asistencia de la secretaria técnica del Procedimiento Administrativo Disciplinario (PAD).

X. ANEXOS

Anexo N° 1: 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 044-2020-PCM que declara el estado de emergencia nacional.
Anexo N° 2: Constancia de Pago
Anexo N° 3: Verificación de la firma digital
Anexo N° 4: Glosario de término

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.

RENIEC – REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL | Identidad digital

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 044-2020-PCM QUE DECLARA EL ESTADO DE EMERGENCIA NACIONAL

El Suscrito,

RAUL [redacted]

Identificado (a) con DNI N° [redacted], con fecha de emisión [redacted] (verificar fecha de emisión en su DNI físico).

Nombre de la Entidad: ORGANISMO TÉCNICO DE LA ADMINISTRACIÓN DE LOS SERVICIOS DE SANEAMIENTO

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

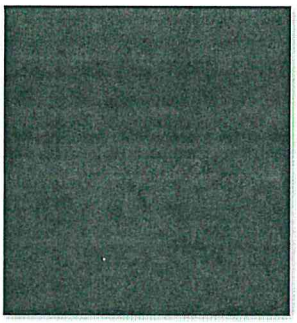
Sede Laboral: TUMBES

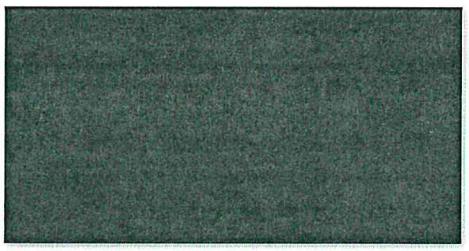
Departamento: TUMBES Provincia: TUMBES

Distrito: TUMBES

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.





IMPORTANTE: La firma debe ser la más parecida a la suscrita en su DNI, caso contrario el trámite será denegado. No se deben colocar sellos, solo la firma.

Lugar y fecha: Tumbes, 21 de junio del 2022

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.

GERENCIA GENERAL – Agua Tumbes – V°B°

GERENCIA DE ADMINISTRACIÓN – Agua Tumbes – V°B°

JEFE DE OFICINA DE ASESORÍA JURÍDICA – Agua Tumbes – V°B°

ANEXO N° 02:

Constancia de Pago de Tasas

Banco de la Nación
el banco de todos

RUC: 20100030595

pagalo.pe
www.pagalo.pe

CONSTANCIA DE PAGO DE TASAS

NRO. TICKET: 220003633034

Datos de la operación : FECHA DE OPERACIÓN: 24/05/2022 20:02:39

ENTIDAD:	RENIEC
TASA/TRIBUTO:	00529 - Emisión De Certificados Digitales Para Entidades De La Administración Pública
CONCEPTO:	Emisión de certificados digitales para el suscriptor

Datos del contribuyente:

TIPO DE DOCUMENTO:	R.U.C
NRO. DE DOCUMENTO:	20103448591

Otros datos :

CANTIDAD:	00001
COSTO UNITARIO:	S/ **********8.10

IMPORTE TOTAL: S/ **********8.10

Secuencia de pago	Fecha de Operación	Trx	Cód. Cajero	Cód. Oficina	Hora de operación
087397-6	24MAY2022	3586	9177	0987	20:02:39

GERENCIA GENERAL Agua Tumbes V°B°

JEFE DE OFICINA DE ADMINISTRACIÓN Agua Tumbes V°B°

JEFE DE OFICINA DE ASESORÍA JURÍDICA Agua Tumbes V°B°

ANEXO N° 03:

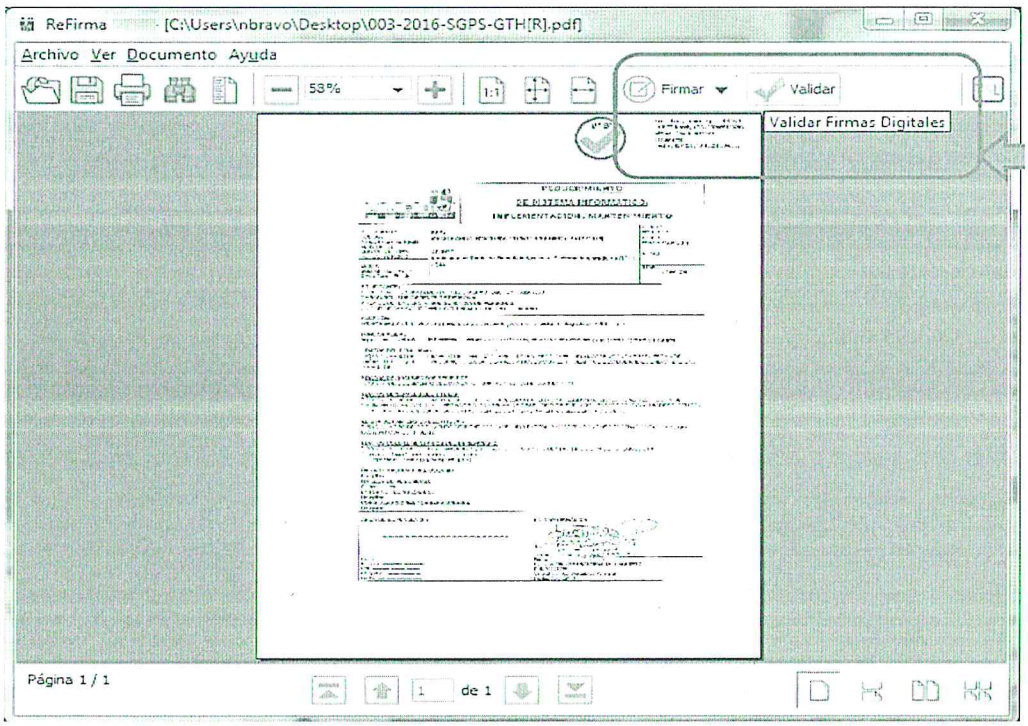
Procedimiento para verificación de la firma digital

El ReFirma PDF tiene la capacidad de efectuar la verificación de la validez de las firmas digitales existentes en el Documento PDF, según lo regulado por la Guía de Acreditación de Aplicaciones de Software emitida por el INDECOPI, para lo cual se deben seguir los siguientes pasos:

PASO 1

Para verificar la integridad y autenticidad de las firmas digitales de un Documento PDF firmado digitalmente, hacer clic sobre el icono Verificar

Figura 1: Pantalla Principal con el Documento PDF firmado digitalmente



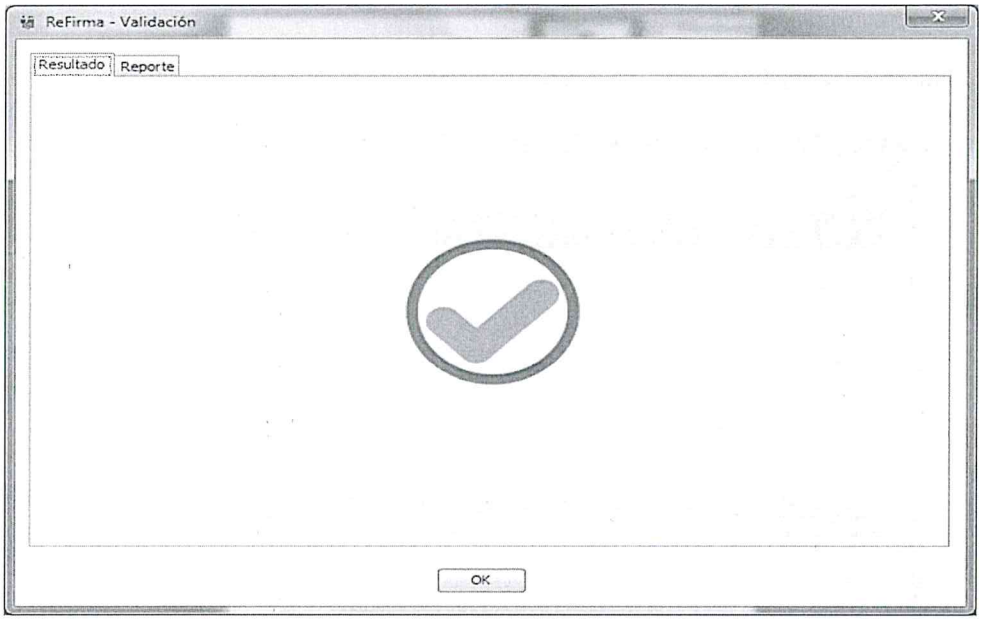
La aplicación procede a verificar la firma digital, lo cual demora unos segundos.

A continuación, aparece una ventana que contiene 04 pestañas, las cuales muestran los resultados de la verificación.

PASO 2

Al aparecer la ventana **ReFirma PDF – Resultado de la Verificación** (ver Figura), en la pestaña **Resultado**, por defecto se aprecia que el Documento PDF contiene una o múltiples Firmas Digitales válidas.

Figura 2: ReFirma PDF – Resultado de la verificación

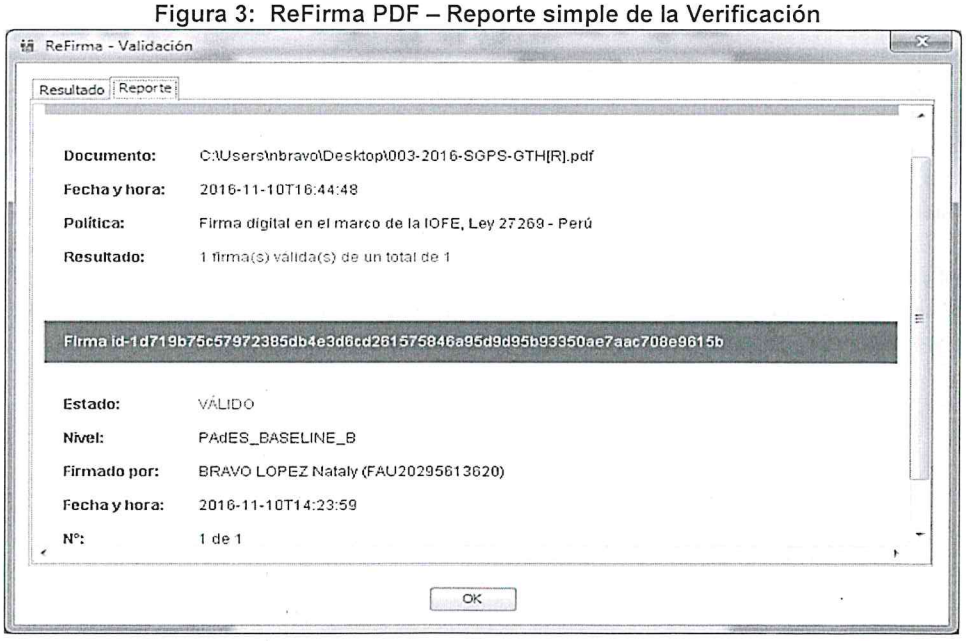


Nota 1.
La ventana de la Figura es la misma que se visualiza cuando se trata de verificar la validez de una o múltiples firmas en el Documento PDF.

PASO 3

En la ventana **ReFirma PDF – Resultado de la Verificación**, particularmente en la Pestaña **Reporte simple**, se puede visualizar las características generales del Documento PDF firmado digitalmente, tal como se aprecia en la Figura siguiente:

Figura 3: ReFirma PDF – Reporte simple de la Verificación



Nota 2.

Cuando el Documento PDF contiene varias firmas digitales, y se ha realizado la verificación de la validez de la firma, se tendrá por ejemplo para 03 firmas digitales, la siguiente ventana:

Figura 4: Verificación de la Validez de 03 Firmas Digitales en un Documento PDF

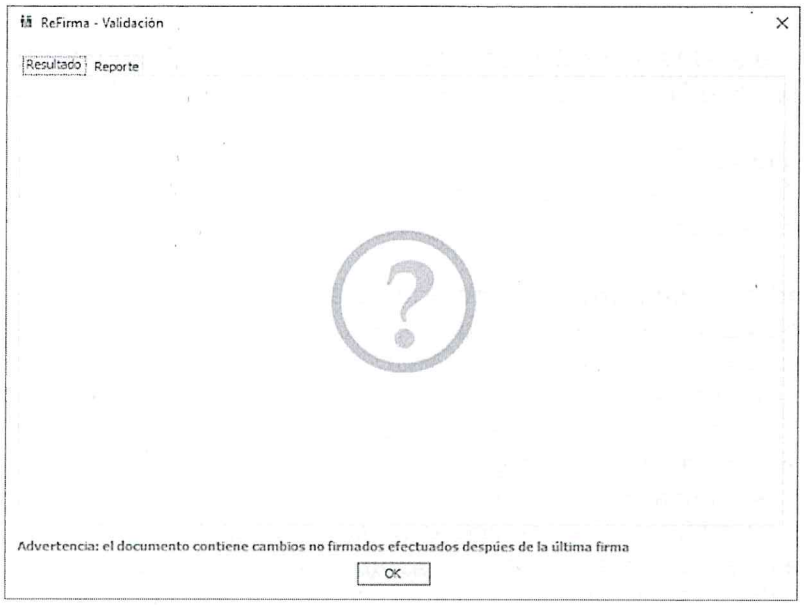
Nota 3.

En el **ejemplo** de la Figura 3 y 4, no se dispone del servicio Sellado de Tiempo activo.

Nota 4.

En caso, un Documento PDF firmado digitalmente haya sido modificada, producto del proceso de verificación de la validez de la firma digital se tendrá la siguiente pantalla:

Figura 5: ReFirma PDF – Resultado de la verificación: Documento PDF firmado digitalmente alterado



Referencia: uso del software refirma PDF (RENIEC)

ANEXO N° 4

Glosario de términos

1. **Administrador del Certificado Digital:** Es el servidor designado por el Gerente General, será el responsable en Coordinar las Gestiones de Certificados Digitales ante el Registro Nacional de Identificación y Estado Civil - RENIEC.

2. **Autenticación:** Proceso que permite determinar la identidad del firmante, en función del documento electrónico firmado digitalmente por éste, garantizando su vinculación e integridad.

3. **Autoridad administrativa competente:** Es el organismo público responsable de acreditar las Entidades de Certificación, a las Entidades de Registro o Verificación y a los Prestadores de Servicios de Valor Añadido, públicos y privados, encargadas de reconocer los estándares tecnológicos aplicables en la Infraestructura Oficial de Firma Electrónica, de supervisar dicha Infraestructura y de cumplir las demás funciones señaladas en el reglamento de la Ley N° 27269, Ley de Firmas y Certificados Digitales aprobado con Decreto Supremo N° 052-2008-PCM, o aquellas que requiera en el transcurso de sus operaciones, conforme a la normativa que le resulte aplicable. Dicha responsabilidad recae en el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual – INDECOPI.

4. **Certificado Digital:** Es un 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.

5. **Contraseña:** Código o combinación de caracteres, utilizado como medida de seguridad y cuyo objeto es el de proteger el "acceso no autorizado" a un recurso determinado.

6. **Clave privada:** Es una de las claves de un sistema de criptografía asimétrica que es usada para generar una firma digital en un documento electrónico para firmar un documento. La clave privada sólo debe permanecer en propiedad del suscriptor.

7. **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.

8. **Documentos:** Son los escritos públicos o privados, los impresos, fotocopias, facsímil o fax, planos, cuadros, dibujos, fotografías, radiografías, cintas cinematográficas microformas tanto en la modalidad de microfilm como en la modalidad de soportes informáticos y otras reproducciones de audio, video, la telemática en general y demás objetos que recojan contengan o representen algún hecho, o una actividad humana o su resultado.

9. **Documento electrónico:** Es la unidad básica documentaria cuyo soporte material es algún tipo de dispositivo electrónico o magnético, susceptible de ser generada, clasificada, gestionada, transmitida, procesada o conservada por una persona natural o jurídica utilizando sistemas informáticos.

10. **Entidad de Certificación:** Es la persona jurídica pública o privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros

servicios inherentes a la certificación digital. Asimismo, puede asumir las funciones de registro verificación. Para el Estado Peruano es el Registro Nacional de Identificación y Estado Civil – RENIEC.

11. **Entidad de Registro o Verificación (EREP):** Es la persona jurídica, con excepción de los notarios públicos, encargada del levantamiento de datos, la comprobación de éstos respecto a un solicitante de un certificado digital, la aceptación y autorización de las solicitudes para la emisión y cancelación. De acuerdo al Reglamento de la Ley N° 27269, Ley de Firmas y Certificados Digitales aprobado con Decreto Supremo N° 052-2008-PCM, el RENIEC es la única entidad de certificación, verificación y registro en nuestro país.

12. **Equivalencia funcional:** Principio por el cual los actos jurídicos realizados por medios electrónicos que cumplan con las disposiciones legales vigentes poseen la misma validez y eficacia jurídica que los actos realizados por medios convencionales, pudiéndoles sustituir para todos los efectos legales. De conformidad con lo establecido en la Ley y su Reglamento, los documentos firmados digitalmente pueden ser presentados y admitidos como prueba en toda clase de procesos judiciales y procedimientos administrativos.

13. **Expediente:** Conjunto de documentos que acumulan toda la actividad procedimental de un mismo asunto originado de oficio o a solicitud de los administrados.

14. **Firma Digital:** Es aquella firma electrónica que utilizando una técnica de criptografía asimétrica, permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su control, 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, siempre y cuando haya sido generada por un Prestador de Servicios de Certificación Digital, debidamente acreditado, que se encuentre dentro de la Infraestructura Oficial de Firma Electrónica (IOFE) de Perú.

15. **Firma electrónica:** La firma electrónica se realiza mediante un procedimiento igual al de la firma digital pero el certificado digital no es emitido dentro del marco de la Infraestructura Oficial de Firma Electrónica (IOFE) de Perú.

16. **Firma principal:** Es la firma digital del autor del documento o del funcionario que suscribe el documento electrónico.

17. **Firma visto bueno:** Es la firma digital del asesor, especialista, asistente, colaborador, servidor o funcionario, quien elaboró, verificó, controló o revisó el documento. Puede incluir también la firma digital del llamado por procedimiento a dar confianza administrativa a quién suscribe la firma principal del documento electrónico.

18. **Infraestructura Oficial de Firma Electrónica:** Es un 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.

    La identidad de su autor: Lo que es regulado conforme a Ley. El sistema incluye la generación de firmas digitales, en la que participan entidades de certificación y entidades de registro o verificación acreditadas ante la Autoridad Administrativa

Competente, incluyendo a la Entidad de Certificación Nacional para el Estado Peruano, las Entidades de Registro o Verificación para el Estado Peruano y los Prestadores de Servicios de Valor Añadido para el Estado Peruano.

19. **Integridad:** Presunción legal por la cual un documento electrónico no ha sido alterado desde su emisión hasta su recepción. Es decir, se presume que el mensaje de datos recibido corresponde al enviado. Por esta presunción, un documento electrónico firmado digitalmente conforme a las normas vigentes conserva la integridad del mensaje de datos, por el hecho de haber sido firmadas digitalmente, sin importar en que medio quede almacenado.

20. **No repudio:** Cuando una persona firma digitalmente un documento electrónico (al igual que cuando lo hace con una firma manuscrita) materializa en este acto la expresión de su voluntad, vinculando a la persona con el contenido del documento. De esta forma la persona no puede repudiar posteriormente la manifestación de su voluntad. El documento es veraz y sus efectos plenos.

21. **Pin:** Es un número de identificación personal utilizado como contraseña para acceder de manera segura a ciertos sistemas informáticos.

22. **Presunción de veracidad:** Todos los documentos generados en los sistemas con firma digital integrada en todas las formas y formalidades prescritas, responden a la verdad de los hechos que ellos afirman.

23. **Representante del titular:** Persona natural que cuenta con facultades para representar a la persona jurídica en los trámites de certificado digital ante la EREP-RENIEC.

24. **Suscriptor:** Es la persona natural responsable de la generación y uso de la clave privada, a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente.

25. **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 RENIEC.