"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la Universalización de la Salud"

DIRECTIVA Nº 002-2020-INAIGEM/GG

"NORMAS PARA LA SOLICITUD Y USO DEL CERTIFICADO Y FIRMA DIGITAL PARA LOS SUSCRIPTORES Y DOCUMENTOS EN EL INAIGEM"

Versión	1.0

ROL	ÓRGANO	SELLO Y FIRMA
Formulada por	**Oficina de Tecnologías de la Información**	INAIGEM V.B Digital Firmado digitalmente por LEZCANO BALAREZO David FAU 20600404262 soft Motivo: Doy V° B° Fecha: 03.08.2020 18:16:03 -05:00
Revisada por	**Oficina de Planeamiento, Presupuesto y Modernización** **Oficina de Asesoría Jurídica**	INAIGEM V.B Digital Firmado digitalmente por CHACALCAJE ELIAS Jesus Santiago FAU 20600404262 soft Motivo: Doy V° B° Fecha: 04.08.2020 16:51:27 -05:00 INAIGEM V.B Digital Firmado digitalmente por ROJAS GUTIERREZ Guillermo Arturo FAU 20600404262 soft Motivo: Doy V° B° Fecha: 03.08.2020 10:51:55 -05:00
Aprobada por	**Gerencia General**	INAIGEM V.B Digital Firmado digitalmente por SAAVEDRA ESPINOZA Victor Angel FAU 20600404262 soft Motivo: Doy V° B° Fecha: 03.08.2020 00:56:47 -05:00

HUARAZ – PERÚ

PRESENTACIÓN

Mediante Ley N° 30286, se crea el Instituto Nacional de Investigación en Glaciares y Ecosistemas de Montaña (INAIGEM) como organismo técnico especializado adscrito al Ministerio del Ambiente, con personería jurídica de derecho público con competencia a nivel nacional y autonomía administrativa, funcional, técnica, económica y financiera que constituye un pliego presupuestal, con la finalidad de fomentar y expandir la investigación científica y tecnológica en el ámbito de los glaciares y ecosistemas de montaña, promoviendo su gestión sostenible en beneficio de las poblaciones que viven en o se benefician de dichos ecosistemas, constituyéndose en la máxima autoridad en investigación científica de los glaciares y ecosistemas de montaña, sin perjuicio de las competencias y funciones específicas asignadas a otros organismos del Estado.

Mediante la Ley Nº 27269, modificada por la Ley Nº 27310, se aprobó la Ley de Firmas y Certificados Digitales, que regula la utilización de la firma digital otorgándole la misma validez y eficacia jurídica que la firma manuscrita u otra análoga, estableciéndose los lineamientos generales respecto de los Prestadores de Servicios de Certificación Digital y la necesidad de contar con una Autoridad Administrativa Competente encargada de regular de manera más específica esta materia

Mediante el Decreto Supremo Nº 019-2002-JUS, modificado por el Decreto Supremo Nº 024-2002-JUS, se aprobó el Reglamento de la Ley Nº 27269 - Ley de Firmas y Certificados Digitales, el cual finalmente fuera derogado mediante Decreto Supremo Nº 004-2007-PCM, publicado en el Diario Oficial El Peruano con fecha 14 de enero de 2007, que aprobó el Reglamento de la Ley de Firmas y Certificados Digitales.

El Estado Peruano, en el marco de la Infraestructura Oficial de Firma Electrónica (IOFE), otorgó al RENIEC el rol de ECERNEP, ECEP y EREP, y en consecuencia la facultad de emitir certificados digitales para personas naturales y jurídicas que lo soliciten.

En ese marco se ha elaborado la presente directiva, con la finalidad de contar con un instrumento a nivel institucional que regule la solicitud y uso del certificado y firma digital para los suscriptores y documentos en el INAIGEM.

DIRECTIVA Nº 002-2020-INAIGEM/GG

INDICE

Contenido **Página N°**

DIRECTIVA N° 002-2020-INAIGEM/GG

"NORMAS PARA LA SOLICITUD Y USO DEL CERTIFICADO Y FIRMA DIGITAL PARA LOS SUSCRIPTORES Y DOCUMENTOS EN EL INAIGEM"

CAPITULO I
DISPOSICIONES PRELIMINARES

Artículo 1. Objeto

Establecer disposiciones internas para la autorización, uso, renovación y cancelación de certificados y firmas digitales de los suscriptores del Instituto Nacional de Investigación en Glaciares y Ecosistemas de Montaña (INAIGEM).

Artículo 2. Finalidad

Contar con un instrumento técnico a nivel institucional que regule los procedimientos para conocer las disposiciones generales respecto al uso del certificado digital, lograr que los suscriptores soliciten el alta de la firma digital, la renovación, y al término de sus funciones en la Entidad se solicite la baja del mismo.

Artículo 3. Alcance

Las disposiciones establecidas en la presente directiva serán de obligatorio cumplimiento por los todos trabajadores de los Órganos y Unidades Orgánicas del INAIGEM y del/la Titular del Certificado Digital de INAIGEM para asumir su representación ante las autoridades administrativas, así como para los suscriptores de INAIGEM.

Artículo 4. Base Legal

4.1 Ley Nº 30286, Ley que crea el Instituto Nacional de Investigación en Glaciares y Ecosistemas de Montaña – INAIGEM.

4.2 Ley Nº 27269, Ley de Firmas y Certificados Digitales, y su Reglamento, aprobado por Decreto Supremo Nº 052- 2008 – PCM.

4.3 Decreto Legislativo N° 295 por el cual se promulga el Código Civil

4.4 Decreto Legislativo N° 681, Normas que regulan el uso de tecnologías avanzadas en materia de archivo de documentos e información tanto respecto a la elaborada en forma convencional cuanto la producida por procedimientos informáticos en computadoras, y sus modificatorias, y su Reglamento, aprobado mediante Decreto Supremo N° 009-92-JUS, y sus modificatorias.

4.5 Decreto Legislativo Nº 1412, que aprueba la Ley de Gobierno Digital.

4.6 Decreto Legislativo Nº 1310, que aprueba medidas adicionales de simplificación administrativa.

4.7 Decreto Supremo N° 004-2013-PCM, se aprobó la Política Nacional de Modernización de la Gestión Pública, la cual establece al Gobierno Electrónico como uno de los tres ejes transversales en los que se apoyaran los Pilares Centrales de la Política Nacional de Modernización de la Gestión Pública.

4.8 Decreto Supremo Nº 026-2016-PCM, que aprueba medidas para el fortalecimiento de la infraestructura oficial de firma electrónica y la implementación progresiva de la firma digital en el Sector Público y Privado.

4.9 Resolución de Secretaría de Gobierno Digital Nº 001-2017-PCM/SEGDI, que aprueba el Modelo de Gestión Documental en el marco del Decreto Legislativo Nº 1310.

4.10 Resolución de Gerencia General Nº 028-2020-INAIGEM/GG, que designa al jefe de la Oficina de Tecnologías de la Información, como el funcionario que actuará en nombre y representación del INAIGEM, asumiendo las obligaciones del titular estipuladas en el artículo 15, Reglamento de la Ley de Firmas y Certificados Digitales aprobado con Decreto Supremo N°052-2008-PCM.

CAPÍTULO II
DISPOSICIONES GENERALES

Artículo 5. Definiciones.

5.1 Autorización: Es el registro que se efectúa en el sistema administrativo de certificación digital, como consecuencia de la solicitud de emisión de certificados digitales para los suscriptores y el cumplimiento de requisitos.

5.2 Certificado Digital: Documento credencial electrónico generado y firmado digitalmente por una entidad de certificación que vincula un par de claves con una persona natural o jurídica confirmando su identidad**.**

5.3 Clave Privada: 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 de la firma digital.

5.4 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.

5.5 Contrato de prestación de Servicios de Certificación Digital: Contrato de Certificado Clase III – Persona Jurídica, suscrito en fecha 20 de noviembre de 2018 entre el INAIGEM y el RENIEC, mediante el cual la EREP-RENIEC y la ECEP-RENIEC se comprometen a prestar, los Servicios de Certificación Digital, para el uso de autentificación y firma digital a solicitud del INAIGEM.

5.6 Desdecirse: Retractarse y negar una opinión que anteriormente se ha sostenido.

5.7 Dispositivo criptográfico: Es el contenedor físico que permite portar el certificado digital y protege las claves criptográficas. Su uso es indispensable para entornos adecuados de protección de la clave privada del certificado digital.

5.8 Documento Electrónico: Conjunto de datos basados en bits o impulsos electromagnéticos, elaborados, generados, transmitidos, comunicados y archivados a través de medios electrónicos, ópticos o cualquier otro análogo. Deberán ser accesibles para su posterior consulta y conservados en su formato original de generación, envío, recepción u otro formato que reproduzca en forma demostrable la exactitud e integridad del contenido electrónico; y ser conservada la data que permita determinar el origen, destino, fecha y hora de envío. Los documentos internos y externos que se emitan en INAIGEM se generan en formato electrónico a través del software de gestión documental de acuerdo a los tipos documentales normalizados de la directiva “Normas que regulan la gestión documental en el Instituto Nacional de Investigación en Glaciares y Ecosistemas de Montaña – INAIGEM”.

5.9 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 o verificación.

5.10 Entidades de Registro o Verificación para el Estado Peruano (EREP-RENIEC): Son entidades acreditadas por la autoridad administrativa competente, encargadas del levantamiento de datos, comprobación de la información del solicitante, identificación y autentificación de los titulares y suscriptores, aceptación y autorización de solicitudes de emisión, cancelación, modificación, re-emisión y suspensión, si fuera el caso, de certificados digitales además de su gestión ante las entidades de certificación.

5.11 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.

5.12 Firma Visto Bueno: Es la firma digital configurada como un tipo de firma adicional, que corresponderá a cada uno de los firmantes responsables de revisar y dar visto bueno al documento.

5.13 Infraestructura oficial de firma electrónica (IOFE): 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.
- La generación de firmas digitales.

5.14 Integridad: Presunción legal de que un documento, por el hecho de haber sido firmado digitalmente conforme a las normas vigentes, no ha sido alterado desde su emisión hasta su recepción, y de que conserva la integridad del mensaje de datos, sin importar en qué medio quede almacenado.

5.15 Microforma: Es una figura jurídica con un alto componente informático, creada en el Perú para que las imágenes de los documentos digitalizados tengan el mismo valor probatorio que un documento en papel. Conforme a: NTP 392-030-2:2015 MICROFORMAS, Requisitos para las organizaciones que administran sistemas de producción y almacenamiento. Parte 2: Medios de archivo electrónico, 3° Edición, el 31 de diciembre de 2015.

5.16 Microarchivo: Conjunto ordenado y codificado de los elementos materiales de soporte y portadores de microformas grabadas, provistos de sistemas de índice y medios de recuperación que permitan encontrar, examinar visualmente y reproducir en copias exactas los documentos almacenados como microformas

5.17 No repudio: Ésta expresión hace referencia a la vinculación de un individuo (o institución) con el documento electrónico, de tal manera que dicha persona no puede desdecirse de sus actos cuando ha plasmado su voluntad en un documento y lo ha firmado en forma manuscrita o digitalmente con un certificado emitido por una entidad de certificación acreditada en cooperación de una EREP - RENIEC, empleando un software de firma digital acreditado, y siempre que cumpla con lo previsto en la legislación civil.

5.18 PIN: Secuencia numérica que debe ser de único conocimiento del suscriptor que permite que el dispositivo criptográfico realice determinadas operaciones con la clave privada.

5.19 **PUK**: Secuencia de caracteres que permiten el cambio o desbloqueo del PIN. Clave personal de desbloqueo.

5.20 **Proceso de Certificado Digital:** Es el proceso a través del cual se gestiona el certificado digital ante la EREP-RENIEC, que contempla cuatro etapas:

- La suscripción de la solicitud
- Emisión de la solicitud de suscripción
- Remisión de certificado
- Cancelación del certificado digital.

5.21 **Responsable técnico:** Es la persona encargada de instalar los componentes para el uso del certificado digital, custodiar los dispositivos criptográficos y de corresponder hacer entrega del dispositivo criptográfico y de orientar a los suscriptores para el correcto uso de dicho certificado, es el personal de la OTI.

Es el responsable de la custodia y administración de la clave PUK para aquellos dispositivos criptográficos que cuenten con esta opción. A su vez es el responsable del formateo de dispositivos criptográficos los cuales se encuentren bloqueados.

5.22 **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 utilizando su clave privada.

5.23 **Token Criptográfico:** Es un dispositivo de almacenamiento, que tiene una apariencia similar a una memoria USB, que almacena de forma segura y confiable el certificado digital asignado a una persona titular que le permite firmar digitalmente, debiendo cumplir con el estándar FIPS 140-2.

5.24 **Titular del Certificado Digital de INAIGEM:** Es la persona designada para administrar los certificados digitales de la entidad. Es aquel que representa legalmente a la entidad. Adicionalmente, dentro de la plataforma integrada de la entidad de registro o verificación para el estado peruano (EREP-RENIEC), gestiona listas de autorización para los suscriptores, designa un representante alterno; asimismo, realiza las altas y bajas de los certificados digitales de sus suscriptores.

Artículo 6. Siglas o Acrónimos.

Sigla	Denominación
IOFE	Infraestructura oficial de firma electrónica
EREP	Entidad de Registro Digital del Estado Peruano
ECEP	Entidad de Certificación para el Estado Peruano
PIN	Personal Identification Number, es un tipo de contraseña
PUK	Acrónimo de Personal Unlocking Key (también conocido como Personal Unlocking Code o Personal Unlock Key) o Clave Personal de Desbloqueo
FIPS	Norma para el procesamiento de información, describe el cifrado y los requisitos de seguridad relacionados que los productos de TI deben cumplir para el uso con datos sensibles, pero no clasificados.
OTI	Oficina de Tecnologías de la Información.
NTP	Norma Técnica Peruana
RENIEC	Registro Nacional de Identificación y Estado Civil
PDF	Portable Document Format, formato de documento portátil, es un formato de almacenamiento para documentos digitales independiente de plataformas de software o hardware.
INDECOPI	Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad
PCM	Presidencia del Consejo de Ministros

Artículo 7. Consideraciones respecto de la firma digital.

7.1 Validez legal de la firma digital

a) La firma digital generada dentro de la Infraestructura Oficial de Firma Electrónica tiene la misma validez y eficacia jurídica que una firma manuscrita, siempre y cuando haya sido generada por un prestador de servicios de certificación digital debidamente acreditado, y que no medie alguno de los vicios de la voluntad previstos en el Título VIII del Libro II del Código Civil.

b) Para los efectos de la presente directiva, las firmas digitales comprenden tanto la firma principal o visto bueno efectuados en el documento electrónico emitido. Asimismo, un documento electrónico puede contar con una o varias firmas digitales de diferentes suscriptores de INAIGEM.

c) En caso que por la naturaleza del procedimiento se requiera un documento impreso en papel, generado con certificado y firma digital, éste se puede realizar, siendo el impreso una copia simple del mencionado documento electrónico.

7.2 Principios legales de la firma digital

a) **Autenticación**: Es el proceso técnico que permite determinar la identidad de la persona que firma digitalmente, en función del documento electrónico firmado por éste y al cual se le vincula; este proceso no otorga certificación notarial ni fe pública.

b) **Equivalencia Funcional**: Principio por el cual los actos jurídicos realizados por medios electrónicos que cumplan 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 a lo establecido en la Ley N° 27269 Ley de Firmas y Certificados Digitales y su reglamento aprobado mediante Decreto Supremo N° 052-2008-PCM, los documentos firmados digitalmente pueden ser presentados y admitidos como prueba en toda clase de procesos judiciales y procedimientos administrativos.

c) **Integridad**: Es la característica que indica que un documento electrónico no ha sido alterado desde la transmisión por el iniciador hasta su recepción por el destinatario.

d) **Neutralidad Tecnológica**: Es el principio de no discriminación entre la información consignada sobre papel y la información comunicada o archivada electrónicamente; asimismo, implica la no discriminación, preferencia o restricción de ninguna de las diversas técnicas o tecnologías que pueden utilizarse para firmar, generar, comunicar, almacenar o archivar electrónicamente la información.

e) **No Repudio**: Es la imposibilidad para una persona de desdecirse de sus actos cuando ha plasmado su voluntad en un documento y lo ha firmado en forma manuscrita o digitalmente con un certificado emitido por una entidad de certificación acreditada en cooperación de una entidad de registro o verificación acreditada, salvo que la misma entidad tenga ambas calidades, empleando un software de firmas digitales acreditado, y siempre que cumpla con lo previsto en la legislación civil.

7.3 Obligaciones del suscriptor.

a) Entregar información veraz bajo su responsabilidad.
b) Generar la clave privada y firmar digitalmente mediante los procedimientos señalados por la Entidad de Certificación.
c) La clave privada es intransferible. En tal sentido, el suscriptor es responsable de la misma, por lo que deberá mantener su control y la reserva bajo responsabilidad.
d) Observar las condiciones establecidas por la Entidad de Certificación para la utilización del certificado digital y la generación de firmas digitales.
e) En caso de que la clave privada quede comprometida en su seguridad, el suscriptor

debe notificarlo de inmediato al Titular del Certificado Digital de INAIGEM para que éste solicite a la EREP - RENIEC o a la Entidad de Certificación que participó en su emisión, la cancelación del certificado digital.

7.4 Emisión de documentos con firma digital.

a) La documentación electrónica emitida bajo el alcance de la presente directiva es aquella que cuenta con firma digital bajo la Infraestructura Oficial de Firma Electrónica — IOFE, por lo que es considerada con valor legal.

b) El INAIGEM adecuará sus trámites y procedimientos aplicados en sus comunicaciones, tanto con los ciudadanos como con las distintas entidades de la administración pública, a fin de llevarlos a cabo por medios electrónicos; debiendo asegurar en todo momento la disponibilidad de acceso, la integridad, la autenticidad, el no repudio y la confidencialidad de las transacciones realizadas por estos medios, empleando para tales fines los certificados y firmas digitales emitidos dentro de la Infraestructura Oficial de Firma Electrónica, así como canales seguros.

c) En lo posible, se deberá evitar imprimir los documentos electrónicos, como medida de ecoeficiencia y preservación de recursos naturales.

d) No obstante, lo señalado en el numeral anterior, en caso los ciudadanos y las entidades de la administración pública requieran información institucional y no cuenten con servicios electrónicos seguros que le permitan el acceso a la información de INAIGEM, se deberá remitir la reproducción del documento digital en medio físico, conforme a lo dispuesto en el Decreto Supremo Nº 026-2016-PCM.

CAPITULO III
DISPOSICIONES ESPECIFICAS

Artículo 8. Designación del/de la titular del certificado digital de INAIGEM.

El/La titular del certificado digital de INAIGEM es designado por el/la Gerencia General mediante la resolución gerencial correspondiente, momento desde el cual podrá iniciar las acciones que le correspondan de acuerdo a ley. Entre sus atribuciones está la de encargarse de la administración de la cuenta. Cabe señalar que la designación antes referida deberá ser puesta a conocimiento del RENIEC, conjuntamente con copia del documento que la aprueba.

Artículo 9. Disposiciones de autorización y obtención del certificado digital para suscriptores.

9.1 De la autorización.

a) El/La responsable del órgano o unidad orgánica del suscriptor de INAIGEM que requiera el otorgamiento y uso del certificado digital solicitará al titular del certificado digital de INAIGEM, mediante el Formato Nº1 del presente documento (en formato PDF firmado por el titular y formato Excel para su trámite inmediato).

b) El/La titular del certificado digital de INAIGEM, evaluará las solicitudes para la emisión de certificados digitales del suscriptor, registrando en caso de aceptación, los datos del solicitante en el sistema administrativo de certificación digital.

c) En caso el formato tenga pendiente el llenado de algún campo obligatorio o incorrecta la información remitida, solicitara las correcciones, para que después de subsanada la observación registre los datos del solicitante en el sistema administrativo de certificación digital.

9.2 Obtención del certificado digital.

Para la obtención de los certificados digitales, el/la titular del certificado digital de INAIGEM deberá remitir la información de los suscriptores conforme a lo dispuesto por el numeral anterior.

a) El/La suscriptor(a), recibirá un correo de la plataforma RENIEC, indicándole que ha sido habilitado como aspirante a suscriptor del INAIGEM, asimismo tendrán un plazo de 30 días hábiles desde la recepción del correo para que se apersone a cualquier oficina autorizada del RENIEC, para proceder a validar su identidad y procesar su solicitud de emisión de certificado digital de persona jurídica. En caso no se apersone, automáticamente será eliminado del sistema y tendrá que solicitarlo nuevamente a través del titular del certificado digital del INAIGEM.

b) El/La suscriptor(a), que se apersone al RENIEC - EREP, deben portar su documento nacional de identidad (DNI) vigente o carnet de extranjería; la RENIEC — EREP procede a la autenticación y registro de los formatos para su firma digital o electrónica y la validación de sus huellas dactilares biométricamente. En los casos de campaña del RENIEC - EREP el procedimiento antes referido podrá ser realizado sin necesidad de acudir a la referida entidad, debiendo ser el RENIEC el que se apersone a las instalaciones de INAIGEM para recabar la firma manuscrita respectiva.

c) Posterior a la autentificación y registro en las oficinas del RENIEC - EREP, el/la suscriptor(a) recibe mediante correo electrónico la dirección URL y los accesos brindados por la RENIEC para la descarga del certificado digital en la PC/USB/TOKEN (pudiendo ser dos correos en caso hayan solicitado certificado de HARDWARE y SOFTWARE), una vez que el/la suscriptor(a) obtenga el correo, debe comunicarse con el responsable técnico para su instalación (OTI). Se tiene 30 días calendario para descargar y generar el certificado digital, caso contrario, se tiene que solicitar nuevamente de acuerdo a las disposiciones de autorización y obtención del certificado digital para los suscriptores según lo indicado en el presente articulo 9; es responsabilidad de/la suscriptor(a) realizar el seguimiento de su certificado digital a través de los correos emitidos por la RENIEC.

d) El/La responsable técnico, previa coordinación con el/la suscriptor(a), de ser el caso, entrega el dispositivo criptográfico con el certificado digital y/o descarga el certificado digital de la ruta enviada por el RENIEC - EREP e instala el software, suscribiéndose el Formato Nº 2 de “Acta de Entrega - Recepción” de la presente directiva, el Formato Nº2 será llenado solo si se entrega el dispositivo criptográfico. El/La suscriptor realiza una prueba de firma digital con el aplicativo instalado y el apoyo del responsable técnico; retirado el responsable técnico el suscriptor se remitirá un correo asimismo con el asunto firma digital y colocara en el contenido su clave respectiva con la finalidad de que en caso de olvido pueda recuperar el acceso (esta última actividad no es obligatoria, pero si recomendable; y es personal, en acto privado). En caso de olvido de clave se tiene que realizar el trámite nuevamente a solicitud del suscriptor.

9.3 Uso del certificado digital para la firma digital por los suscriptores.

a) Los documentos suscritos con firma digital deben ser presentados en formato de archivo PDF, el mismo que permite almacenar la(s) firma(s) digitales correspondientes para su uso posterior.

b) El uso de la firma digital no exime a los órganos del INAIGEM de adjuntar la documentación o sustento según corresponda; ni del cumplimiento de lo establecido por los dispositivos legales vigentes que regulan la firma digital.

c) Los suscriptores/as 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 y no repudio del usuario la firma de cualquier documento electrónico usando su usuario y contraseña.

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

- 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.
- Mantener el control y absoluta reserva de la clave privada bajo su responsabilidad.
- Custodiar su contraseña o PIN de acceso a su clave privada de forma diligente, tomando las precauciones razonables para evitar su pérdida, revelación, modificación o uso no autorizado.
- Dejar de utilizar la clave privada, transcurrido el plazo de vigencia del certificado digital.

9.4 Uso del software de firma digital.

El software de firma digital se encuentra acreditado ante el INDECOPI; de esta manera, se certifica que el software cumple con los requisitos e interactúa directamente con la Infraestructura Oficial de Firma Electrónica (IOFE) de la República del Perú, garantizando que los documentos firmados digitalmente a través del software tengan el mismo efecto legal que una firma manuscrita en un documento físico.

9.5 De las características de la firma digital.

Las características mínimas de la firma digital generada dentro de la Infraestructura Oficial de Firma Electrónica son:

a) Se genera al cifrar el código de verificación de un documento electrónico, usando la clave privada del titular del certificado.

b) Es exclusiva del suscriptor y de cada documento electrónico firmado por éste.

c) Es susceptible de ser verificada usando la clave pública del suscriptor.

d) Su generación está bajo el control exclusivo del suscriptor.

e) Está añadida o incorporada al documento electrónico mismo de tal manera que es posible detectar si la firma digital o el documento electrónico fue alterado

Artículo 10. Renovación del certificado digital para la firma digital por los suscriptores.

10.1 Disposiciones para la renovación del certificado digital.

a) Para la renovación del certificado digital del suscriptor, el requerimiento deberá ser gestionado, a través del responsable de la unidad de organización, quien podrá pedir periódicamente el estado de los certificados personales de los suscriptores de su unidad al titular del certificado digital del INAIGEM para lo cual debe remitir todos los DNI de su personal en consulta en formato Excel.

b) El/La suscriptor es responsable de comunicar la intención al responsable de su unidad de organización de renovar su certificado digital, con 10 días de anticipación como mínimo. El/La responsable del órgano o unidad orgánica remitirá el Formato Nº 4 al titular del certificado digital de INAIGEM, quien procederá a registrar la renovación respectiva ante el RENIEC, después deberá seguir los pasos indicados en el Capítulo III, articulo 9.2 Obtención del certificado digital, por lo cual el suscriptor recibirá los respectivos correos por el RENIEC (con los plazos ya estipulados de 30 días, el primer

correo de notificación para que se apersone a una oficina EREP autorizada del RENIEC y otro(s) correo(s) con la aprobación de solicitud del certificado digital de persona jurídica; con el cual debe comunicarse con el responsable técnico, el cual descargará, generará e instalará el certificado digital).

Artículo 11. Cancelación del certificado digital.

11.1 Disposiciones para la cancelación del certificado digital.

a) Para la cancelación del certificado digital de suscriptor, éste deberá de ser, a través del responsable de su órgano o unidad orgánica, quien debe comunicar dicha intención al/a la titular del certificado digital de INAIGEM, quien procederá a registrar la cancelación respectiva ante el RENIEC, según Formato Nº 3 de la presente directiva.

b) El/La suscriptor también podrá tramitar la cancelación de su certificación digital directamente, previa coordinación con el responsable de su órgano o unidad orgánica y el/la titular del Certificado Digital de INAIGEM, apersonándose al RENIEC — EREP portando su documento nacional de identidad vigente ò carnet de extranjería, luego de ello, el RENIEC — EREP informará al titular del certificado digital de INAIGEM vía correo electrónico y/o documento físico de dicha cancelación, quien procederá a informar sobre ello al responsable técnico (OTI).

c) La cancelación del certificado digital del suscriptor conlleva a la devolución de los bienes que hubieren sido entregados al/a la titular del certificado digital de INAIGEM (token de seguridad, entre otros) para el uso del mismo, de ser el caso.

d) En el caso que el suscriptor renuncie o cese se deberá cancelar su certificado digital jurídico, devolver el token al responsable técnico, deberá incluir la presentación del Formato N° 3 acta de cancelación del certificado digital debidamente llenado y firmado, el mismo que deberá ser remitido al titular del certificado digital de INAIGEM para la cancelación del certificado digital del suscriptor en el sistema administrativo de certificación digital del RENIEC - EREP.

11.2 Registro y actualización de las altas y bajas de suscriptores

El/La titular del certificado digital debe llevar un registro actualizado de las autorizaciones y cancelaciones de certificados digitales de los suscriptores, cabe mencionar que el responsable del órgano o unidad orgánica, debe comunicar las cancelaciones o no renovación de los suscriptores.

11.3 Pérdida o Robo del token criptográfico y certificado digital

El/La suscriptor está en la obligación de comunicar al responsable de su órgano o unidad orgánica, la cancelación y la emisión de un nuevo certificado digital de suscriptor a su cargo ante la Entidad de Registro o Verificación para el Estado Peruano (EREP).

Para tal efecto, el responsable del órgano o unidad orgánica gestionará la adquisición del token criptográfico para el/la suscriptor a su cargo, previa presentación de la copia simple de la denuncia policial y copia simple del DNI.

11.4 Bloqueo del token criptográfico por superar el límite de intentos de acceso

El/La suscriptor del certificado digital que supere el límite de intentos de acceso al token criptográfico, está en la obligación de comunicar el bloqueo al responsable técnico, el número de intentos depende de la marca del token. En caso el/la responsable técnico no pueda desbloquear el token, indicará al suscriptor realice la solicitud del certificado digital de acuerdo a lo establecido en el Capítulo III Artículo 9. Disposiciones de autorización y obtención del certificado digital para suscriptores.

Artículo 12. De la conservación de documentos electrónicos.
Cuando los documentos, registros o informaciones requieran de una formalidad para la conservación de documentos electrónicos firmados digitalmente, deberán:

a) Ser accesibles para su posterior consulta.

b) Ser conservados con su formato original de generación, envío, recepción u otro formato que reproduzca en forma demostrable la exactitud e integridad del contenido electrónico.

c) Ser conservado todo dato que permita determinar el origen, destino, fecha y hora del envío y recepción.

Para estos casos, los documentos electrónicos deberán ser conservados mediante microformas o microarchivos, observando para ello lo regulado en el Decreto Legislativo Nº 681 y normas complementarias y reglamentarias; siendo, en tales supuestos, indispensable la participación de un notario o fedatario que cuente con diploma de idoneidad técnica y se encuentre registrado ante su correspondiente colegio o asociación profesional conforme a lo establecido por el Reglamento de la Ley de Firmas y Certificados Digitales.

Artículo 13. De los niveles de seguridad

A fin de garantizar el cumplimiento de los requerimientos de seguridad necesarios para la implementación de los componentes y aplicaciones de la Infraestructura Oficial de Firma Electrónica y en concordancia con el Reglamento de la Ley de Firmas y Certificados Digitales se establecen tres niveles:

a) Medio
b) Medio Alto
c) Alto (Entidades Militares)

CAPÍTULO IV
DISPOSICIONES COMPLEMENTARIAS

Artículo 14. DISPOSICION COMPLEMENTARIA TRANSITORIA

ÚNICA. Por la naturaleza de la utilización de las firmas y certificados digitales, lo dispuesto en la presente norma será ejecutado progresivamente de acuerdo a las disposiciones que se emitan sobre la materia, con la finalidad de que no dificulte su labor administrativa o procedimental en un inicio.

CAPÍTULO V
RESPONSABILIDADES

Artículo 15° RESPONSABILIDADES GENERALES

Artículo 15.1. De la OTI

a) La Oficina de Tecnologías de la Información es responsable de ejecutar las acciones necesarias en el ámbito de su responsabilidad, a fin de difundir y brindar la asistencia técnica a las unidades de organización comprendidas en el alcance de la presente directiva.

b) Llevará el registro del personal autorizado del INAIGEM que realizó las gestiones del certificado y firma digital a través de su representante el titular del certificado digital.

c) Es responsable de mantener en los equipos de cómputo de los usuarios correspondientes las configuraciones necesarias con fines de uso y almacenamiento.

d) Orientar a los suscriptores en el uso de software correspondiente.

Artículo 15.2 De los jefes y/o directores de órganos y unidades orgánicas.

a) Los funcionarios a cargo de los órganos y/o unidades orgánicas en el alcance de la presente directiva son los responsables de velar por el cumplimiento de las disposiciones para el uso de la firma digital en documentos electrónicos oficiales.

b) El Jefe(a) / Director(a) de cada órgano, unidad orgánica será quien designará el uso del token criptográfico del suscriptor de acuerdo a sus funciones.

Artículo 15.3 Del Suscriptor

a) El/La suscriptor es responsable de hacer el seguimiento correspondiente al trámite de solicitud, renovación y cancelación del certificado y firma digital, por lo que le corresponde al suscriptor una vez recibo el correo por la entidad correspondiente RENIEC comunicarse con el responsable técnico.

b) Efectuar la firma exclusivamente en los documentos autorizados de INAIGEM, bajo responsabilidad.

c) A partir de la recepción del certificado digital para la firma digital, los suscriptores de INAIGEM reconocen como propios y auténticos los documentos que por su medio se generen, y aceptan las consecuencias derivadas del uso de la firma digital que expresa la manifestación de su voluntad para todo efecto legal, siendo responsables de la veracidad del contenido de la información registrada en todos los documentos autorizados.

d) Al ser responsables de los trámites y actuaciones que se realicen utilizando su firma digital, deberán evitar que terceras personas utilicen las claves asignadas.

e) En caso de olvido del PIN o contraseña, deberán informarlo inmediatamente al jefe(a) / director(a) de su unidad orgánica o órgano y al responsable técnico para impulsar las acciones para la revocación de su certificado y el trámite de uno nuevo.

f) El/La suscriptor es responsable de la renovación de su firma digital, el cual tiene vigencia de 1 año, en caso el/la suscritor no solicite su renovación dentro de este periodo no podrá realizar la firma digital de ningún documento hasta gestionar la misma.

ANEXOS

Anexo N°01 Formatos del Certificado y Firma Digital

Anexo N°02 Flujograma para la obtención del Certificado Digital.

INAIGEM INSTITUTO NACIONAL DE INVESTIGACIÓN EN GLACIARES Y ECOSISTEMAS DE MONTAÑA

ANEXO 01: FORMATOS DEL CERTIFICADO Y FIRMA DIGITAL

FORMATO N°1

FORMATO DE AUTORIZACION PARA LA EMISION DE CERTIFICADOS DIGITALES A LOS SUSCRIPTORES

(*) = CAMPOS OBLIGATORIOS; USUARIO: NOMBRES Y APELLIDOS, VERIFICAR QUE LOS CAMPOS DNI, TELEFONO Y ANEXO TENGAN SOLO NÚMEROS NO GUIONES, CANTIDAD MAXIMA DE FILAS 50 POR PAGINA; REMITIR EN FORMATOS (PDF FIRMADO Y EN EXCEL)

(**) = SELECCIONAR UNA SOLA OPCION, CAMPO OBLIGATORIO

Nº	NACIONALIDAD(*)	NOMBRES (*)	PRIMER APELLIDO(*)	SEGUINDO APELLIDO(*)	DNI (*)	DIRECCIÓN LABORAL (*)	CARGO	ÁREA	TELÉFONO (*)	ANEXO	EMAIL INSTITUCIONAL (*)	TIPO DE CERTIFICADO (**) -Firma Digital y Autenticación. -Cifrado	MODO DE DESCARGA CERTIFICADO (**) -SOFTWARE (PC, laptop) -HARDWARE (token, Smart card)

FORMATO N° 2

ACTA DE ENTREGA – RECEPCION

CONCEPTO	
SUSCRIPTOR	Yo,……., con cargo ……., con DNI Nº …… con correo electrónico institucional ……., recibo los bienes accesorios necesarios para la generación de la firma digital, que son entregados por el responsable técnico de INAIGEM, los mismos que se detallan en el siguiente cuadro (RELACION DE BIENES ENTREGADOS PARA LA GENERACION DE FIRMA DIGITAL)
COMPROMISOS DEL SUSCRIPTOR	Hacer uso adecuado del bien entregado, cuidarlo y conservarlo en buen estado. En caso de renuncie o cese se deberá cancelar su certificado digital jurídico, y devolver el bien al responsable técnico.
PERDIDA DE LOS BIENES DE LA FIRMA DIGITAL	Ante la pérdida del dispositivo criptográfico, se debe presentar: Copia de la denuncia policial y copia del DNI. Asimismo, deberá solicitar la cancelación del certificado digital al titular del certificado de INAIGEM.
DE INAIGEM	No se responsabiliza, cuando el suscriptor realice el traspaso de la tarjeta de firma digital a terceras personas.

RELACION DE BIENES ENTREGADOS PARA LA GENERACION DE FIRMA DIGITAL

(*) CAMPOS OBLIGATORIOS

DENOMIINACION DEL BIEN (*TOKEN)	CODIGO	ESTADO FISICO EN EL QUE SE ENCUENTRA: -CONFORME -INCONFORME	FECHA DE ENTREGA (*)

Firma del/de la Suscriptor/a

Firma del Responsable Técnico (OTI)

ANEXO 01: FORMATOS DEL CERTIFICADO Y FIRMA DIGITAL

FORMATO N°3

FORMATO DE CANCELACION DE CERTIFICADOS DIGITALES – SUSCRIPTORES

(*) = CAMPOS OBLIGATORIOS; VERIFICAR QUE LOS CAMPOS DNI, TELEFONO Y ANEXO TENGAN SOLO NÚMEROS, NO GUIONES; CANTIDAD MAXIMA DE FILAS 50 POR PAGINA; REMITIR EN FORMATOS (**PDF FIRMADO Y EN EXCEL**)

(**) = SELECCIONAR UNA SOLA OPCION, CAMPO OBLIGATORIO

Nº	NACIONALIDAD(*)	NOMBRES (*)	PRIMER APELLIDO(*)	SEGUINDO APELLIDO(*)	DNI (*)	DIRECCIÓN LABORAL (*)	CARGO	ÁREA	TELÉFONO (*)	ANEXO	EMAIL INSTITUCIONAL (*)	FECHA DE CANCELACION (*)	TIPO DE CERTIFICADO CANCELADO (**) -SOFTWARE (PC, laptop) -HARDWARE (token, Smart card)

Firma del titular del órgano

Fecha:

PERÚ

Ministerio del Ambiente

Instituto Nacional de Investigación en Glaciares y Ecosistemas de Montaña

ANEXO 01: FORMATOS DEL CERTIFICADO Y FIRMA DIGITAL

FORMATO N°4

FORMATO DE RENOVACION DE CERTIFICADOS DIGITALES A LOS SUSCRIPTORES

(*) = CAMPOS OBLIGATORIOS; USUARIO: NOMBRES Y APELLIDOS, VERIFICAR QUE LOS CAMPOS DNI, TELEFONO Y ANEXO TENGAN SOLO NÚMEROS, CANTIDAD MAXIMA DE FILAS 50 POR PAGINA; REMITIR EN FORMATOS (PDF FIRMADO Y EN EXCEL)

(**) = SELECCIONAR UNA SOLA OPCION, CAMPO OBLIGATORIO

N°	NACIONALIDAD(*)	NOMBRES (*)	PRIMER APELLIDO(*)	SEGUNDO APELLIDO(*)	DNI (*)	DIRECCIÓN LABORAL (*)	CARGO	ÁREA	TELÉFONO (*)	ANEXO	EMAIL INSTITUCIONAL (*)	TIPO DE CERTIFICADO (*) -Firma Digital y Autenticación	MODO DE DESCARGA CERTIFICADO (**) -SOFTWARE (PC, laptop) -HARDWARE (token, Smart card)

Firma del titular del órgano

Fecha:

ANEXO 02 FLUJOGRAMA PARA LA OBTENCIÓN DE CERTIFICADO DIGITAL