



Política de Privacidad

ECERNEP
ECEP- RENIEC
EREP - RENIEC

Versión: 4.0	Año: 2017	
Elaborado por: Oficial de Privacidad de Datos.	Revisado por: Subgerencia de Regulación Digital de la GRCD	Aprobado por: Gerente de Registros de Certificación Digital

Historial de Cambios				
Ver.	Fecha	Descripción	Responsable	Estado
1.0	22/06/2012	Elaboración y Aprobación	GCRD	Aprobado
2.0	20/11/2012	Se recoge observaciones del evaluador de INDECOPI.	GCRD	Aprobado
3.0	05/07/2013	Actualización	GCRD	Aprobado
4.0.	20/06/2017	Inclusión de Disposiciones aplicables a la ECERNEP y Actualización.	GRCD	Aprobado

- Por resolución Jefatural N° 073-2016/JNAC/RENIEC se aprobó el ROF RENIEC 2016, modificándose la denominación de la gerencia:
Antes: GERENCIA DE CERTIFICACIÓN Y REGISTRO DIGITAL
Ahora: GERENCIA DE REGISTROS DE CERTIFICACIÓN DIGITAL.

POLÍTICA DE PRIVACIDAD

El Registro Nacional de Identificación y Estado Civil (en adelante el RENIEC) es un organismo constitucional y autónomo con personería jurídica de derecho público interno, creado por mandato de la Constitución Política del Perú mediante la Ley N° 26497, goza de atribuciones en materia registral, técnica, administrativa, económica y financiera. Está encargado de organizar y mantener el Registro Único de Identificación de las Personas Naturales e inscribir los hechos y actos relativos a su capacidad y estado civil.

En virtud a lo establecido por la Ley N° 27269 – Ley de Firmas y Certificados Digitales, y por disposición expresa de su vigente Reglamento¹, dentro de la Estructura Jerárquica de Certificación del Estado Peruano incardinada en la Infraestructura Oficial de Firma Electrónica (IOFE), se designó al RENIEC como la única Entidad de Certificación Nacional para el Estado Peruano (ECERNEP), y que actuará también como Entidad de Certificación para el Estado Peruano (ECEP) y Entidad de Registro o Verificación para el Estado Peruano (EREP).

El RENIEC en atención al mandato y encargo confiado y en el cumplimiento de los roles antes indicados, presta sus servicios a las personas naturales y personas jurídicas que mantengan vínculos con el Estado. Para cualquier fin, el domicilio legal del RENIEC es Jr. Bolivia N° 109, Cercado de Lima, Lima 01.

La ECERNEP es la encargada de emitir los certificados raíz para las Entidades de Certificación para Estado Peruano que lo soliciten, así como proponer las políticas y estándares para aquellos y para las Entidades de Registro o Verificación para el Estado Peruano según los requerimientos de la Autoridad Administrativa Competente y de lo establecido en el Reglamento de la Ley de Firmas y Certificados Digitales.

La ECEP-RENIEC es la encargada de la emisión o cancelación de Certificados Digitales, previa autorización de las EREP del RENIEC², así como, de la publicación del Repositorio y de la Lista de Certificados Cancelados (conocida en inglés como Certificate Revocation List, en adelante CRL).

La EREP-RENIEC es la encargada del levantamiento de los datos personales, comprobación de la información presentada por el solicitante, identificación y autenticación de los titulares y suscriptores, autoriza o deniega la solicitud de emisión o cancelación de Certificados Digitales, y gestiona dichas solicitudes ante la ECEP-RENIEC.

Para el RENIEC, la protección de datos personales es un eje primordial y clave dentro de sus actividades y, para proteger de una manera adecuada los datos personales recogidos para los fines de emisión y cancelación de Certificados Digitales, se ha diseñado la presente Política para la ECERNEP, las EREP-RENIEC y la ECEP-RENIEC.

Mediante el presente documento, el RENIEC en sus roles de ECERNEP, de ECEP-RENIEC y de las EREP-RENIEC, informa a todas aquellas personas directa e

¹ Aprobado mediante Decreto Supremo N° 052-2008-PCM, modificado mediante el Decreto Supremo N° 070-2011-PCM, D.S. 105-2012-PCM y el D.S. 026-2016-PCM.

² EL RENIEC se acreditó como EREP para personas naturales según Resolución N° 008-2013/CNB-INDECOPI y como EREP para personas jurídicas según Resolución N° 034-2013/CNB-INDECOPI.

indirectamente involucradas en la actividad de Certificación Digital su Política de Privacidad:

1. OBJETIVO DE LA POLÍTICA DE PRIVACIDAD

La presente Política de Privacidad tiene por objetivo asegurar que el Usuario³ cuente con los instrumentos de juicio necesarios para proporcionar de forma expresa, libre y voluntaria su información personal que se requiere para la prestación del Servicio de Certificación Digital brindado por la ECERNEP, la ECEP-RENIEC, y las EREP-RENIEC; asimismo, informar de manera previa a la recopilación, sobre la finalidad del tratamiento de sus datos, quiénes son o pueden ser sus destinatarios, la existencia de un banco de datos personales, la identidad y domicilio de su titular, el responsable del tratamiento, casos en que procede la transferencia y el tiempo de conservación de sus datos personales, así como, sus derechos, los procedimientos de corrección de su información personal, entre otros.

2. DATOS PERSONALES RECOLECTADOS

La información recopilada es aquella que ha sido proporcionada por el Usuario al momento de solicitar la emisión de un Certificado Digital.

Para la emisión de Certificados Digitales, las EREP-RENIEC en ningún caso recopilan datos personales que revelen el origen étnico o racial, opiniones o convicciones políticas, creencias filosóficas o religiosas o morales, ingresos económicos, afiliación a algún sindicato, salud o vida sexual de sus Usuarios, es decir, los suscriptores y titulares de los mismos. Lo expuesto aplicará para los casos en que la ECERNEP en mérito a sus labores, otorgue el servicio a otras ECEP.

La ECERNEP, ECEP-RENIEC, y las EREP-RENIEC son únicamente responsables de los datos personales proporcionados por el Usuario para fines de la emisión o cancelación de su Certificado Digital, en ningún caso es responsable de la base de datos del Registro Único de Identificación de las Personas Naturales (RUIPN), así como del Registro Civil.

Los Certificados Digitales de los Usuarios contendrán sus datos de identificación, lo cual es avalado por el RENIEC en sus role de ECERNEP, ECEP-RENIEC y las EREP-RENIEC, tanto tratándose de personas naturales como de personas jurídicas.

La ECERNEP, la ECEP-RENIEC y las EREP-RENIEC brindan el nivel de seguridad adecuado en relación a los equipos informáticos y de comunicación utilizados, el personal empleado y los procedimientos utilizados para la autenticación de los datos a ser incluidos en los certificados digitales, en concordancia con las Guías de Acreditación aprobadas por la Autoridad Administrativa Competente.

La ECERNEP dispone de repositorios, accesibles desde la Internet, donde se publican las distintas CRLs, las vigentes y el histórico de éstas, la Política y Declaración de Prácticas de Certificación así como los certificados digitales emitidos por la ECERNEP y los Prestadores de Servicio de Certificación.

³ Para efecto del presente documento entiéndase como Usuario a los titulares y/o suscriptores de certificados digitales. Tratándose de personas naturales, éstas son titulares y suscriptores del certificado digital. En el caso de las entidades de la Administración Pública (personas jurídicas), éstas son titulares del certificado digital, y son suscriptores las personas naturales responsables de la generación y uso de la clave privada, en concordancia con lo dispuesto por el Artículo 9º del Reglamento de la Ley de Firmas y Certificados Digitales.

La ECEP-RENIEC publicará los Certificados Digitales emitidos y cancelados en un Repositorio y en la CRL respectivamente, a fin de que los Terceros que Confían⁴ puedan verificar la validez y estado de su Certificado Digital,

Con relación a los Certificados Digitales, los datos personales en ellos contenidos configuran una fuente accesible al público⁵ y la dirección oficial de correo electrónico de los usuarios podrá ser incorporada en los mismos.

El RENIEC, a través de la ECERNEP, la ECEP-RENIEC, y las EREP-RENIEC, gestionará un banco de datos personales implementado únicamente para los fines de la prestación del Servicio de Certificación Digital.

El RENIEC en sus roles de ECERNEP, ECEP-RENIEC y EREP-RENIEC, por disposición expresa del Reglamento de la Ley de Firmas y Certificados Digitales⁶, mantendrá la información relativa a los Certificados Digitales por un periodo de diez (10) años a partir de la cancelación o expiración de los mismos.

3. PROPÓSITOS DE USO

La información que recopila el RENIEC, en su calidad de Prestador de Servicios de Certificación Digital para el Estado Peruano, se utilizará para el cumplimiento de sus funciones asignadas y para verificar y autenticar la identidad del solicitante y emitir el respectivo Certificado Digital. Asimismo, se utilizará con el propósito de poder brindar a los Usuarios el Servicio de Certificación Digital que solicitaron y para lograr la confianza de los Terceros que Confían.

4. CONCEPTO DE DATO O INFORMACIÓN PERSONAL

De conformidad con lo establecido por la Ley N° 29733 – Ley de Protección de Datos Personales, modificada por Decreto Legislativo N°1353 y su Reglamento, aprobado mediante Decreto Supremo N° 003-2013-JUS, se entiende por “datos personales” a aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados.

5. CONFIDENCIALIDAD Y PROTECCIÓN DE LOS DATOS PERSONALES

El RENIEC en sus roles de ECERNEP, ECEP-RENIEC, y de las EREP del RENIEC ha adoptado medidas de índole organizativas y técnicas que permiten garantizar la seguridad de los datos personales y la información confidencial recibida dentro de la prestación del Servicio de Certificación Digital, evitando su alteración, pérdida, uso o acceso no autorizado.

6. INFORMACIÓN CONFIDENCIAL

⁴ La Décimo Cuarta Disposición Complementaria Final del Reglamento de la Ley de Firmas y Certificados Digitales define como “Tercero que confía o tercer usuario” a las personas naturales, equipos, servicios o cualquier otro ente que actúa basado en la confianza sobre la validez de un certificado y/o verifica alguna firma digital en la que se utilizó dicho certificado.

⁵ Artículo N° 17, numeral 1, del Reglamento de la Ley de Protección de Datos Personales en el que se señala que son fuentes accesibles al público “Los medios de comunicación electrónica, óptica y de otra tecnología, siempre que el lugar en el que se encuentren los datos personales esté concebido para facilitar información al público y esté abierto a la consulta general.”

⁶ Artículo 26, (literal g).

Conforme a lo establecido en las Guías de Acreditación de Entidades de Registro o Verificación y de Certificación, versión 3.3⁷, y el Reglamento de Firmas y Certificados Digitales, el RENIEC mantiene la confidencialidad de la siguiente información:

- a. Material o información reservada de la ECERNEP, ECEP-RENIEC y EREP-RENIEC, incluyendo términos contractuales, planes de negocio e información que verse sobre derechos de propiedad intelectual.
- b. La información del negocio suministrada por la ECEP-RENIEC o por sus proveedores y otras personas con las que la EREP-RENIEC tiene el deber de guardar secreto establecido legal o convencionalmente.
- c. Información que pueda permitir a partes no autorizadas la construcción de un perfil de las actividades de los Usuarios.
- d. Información que pueda permitir a partes no autorizadas establecer la existencia o naturaleza de las relaciones entre los Usuarios o Terceros que Confían.
- e. La causal que motivó la cancelación o revocación de oficio de un Certificado Digital.
- f. Información personal provista por los Usuarios que no sea la autorizada para estar contenida en los Certificados Digitales ni en la CRL.
- g. Toda la documentación contenida en el expediente que custodia la EREP-RENIEC y que no forma parte de la información contenida en el Certificado Digital. Lo expuesto aplicará para los casos en que la ECERNEP en mérito a sus labores, otorgue sus servicios a otras ECEP.
- h. El código de activación del Certificado Digital (código PUK)
- i. Toda la información clasificada como “confidencial”.

7. INFORMACIÓN PÚBLICA - NO CONFIDENCIAL

Los datos personales que serán públicos son aquellos que se incluye en los Certificados Digitales y en la CRL.

Asimismo, se considera no confidencial y por lo tanto accesible por terceros a la siguiente información que se detalla, pero no se limita, a:

- Los Certificados Digitales emitidos por la ECERNEP y ECEP-RENIEC, así como las informaciones contenidas en éstos y el estado de los mismos.
- Certificados Digitales cancelados o revocados de oficio.
- Datos de identidad del Titular y/o Suscriptor que figuran en el Certificado Digital.
- Usos y límites de uso de los Certificados Digitales.

⁷ Numeral 9.3 sobre confidencialidad de la información del negocio y numeral 9.4.2 sobre información tratada como privada.

- Las fechas de emisión y de caducidad del Certificado Digital.
- El número de serie del Certificado Digital.
- Aquella información personal que los Usuarios soliciten o autoricen que se publique.
- La contenida en la Declaración de Prácticas de Registro (RPS).
- La contenida en la Declaración de Prácticas de Certificación (CPS)
- La contenida en la Política de Privacidad.
- La Lista de Certificados Digitales Cancelados o revocados (CRL).
- Toda otra información clasificada como “pública”.

8. REVELACIÓN DE LA INFORMACIÓN CONFIDENCIAL

Excepcionalmente, la información confidencial del Usuario será revelada o comunicada al Poder Judicial cuando una orden judicial así lo exija o cuando ésta sea autorizada, de manera expresa, por el Usuario.

9. MEDIDAS DE SEGURIDAD

El RENIEC mantiene las más estrictas medidas de seguridad respecto de los datos personales y de la información confidencial. Estas medidas se encuentran detalladas en la Política de Seguridad, garantizando de este modo a los Usuarios y Terceros que Confían la disponibilidad, la integridad, autenticidad y confidencialidad de los datos personales recolectados a fin de brindar los servicios de certificación digital.

Para tal efecto, la ECERNEP, la ECEP-RENIEC y las EREP-RENIEC han implementado medidas técnicas y organizativas necesarias para evitar la pérdida, mal uso, alteración, acceso no autorizado y robo de información contenida en nuestro banco de datos personales.

Adicionalmente, es política del RENIEC celebrar acuerdos de confidencialidad con el personal y terceros (contratistas) que tienen acceso a la información clasificada como confidencial, previendo en dicho acuerdo: (i) la obligación de no divulgar cualquier información que pudiera facilitar o coadyuvar a la vulneración de la confidencialidad de la información, aún después de extinguido el vínculo laboral o contractual y, (ii) las consecuencias civiles o penales derivadas de su incumplimiento.

En el supuesto que se vulnere la confidencialidad de los datos personales que no sean públicos o de la información confidencial por parte de algún colaborador (funcionario o servidor) o tercero, el RENIEC iniciará contra los responsables el respectivo procedimiento sancionador, así como las acciones judiciales a que hubiere lugar.

10. DERECHO DE LOS USUARIOS

Los Usuarios podrán ejercer los siguientes derechos:

- Acceder a su información personal. El acceso es gratuito una vez al año.

Solicitar todo tipo de información referente a: ciclo de vida del Certificado Digital, usos del Certificado Digital y procedimientos de acceso y corrección de los datos contenidos en el Certificado, la finalidad del tratamiento de sus datos, el dato de la persona que solicitó la recopilación (si fuera el caso), los organismos de la administración pública a quienes los datos han sido transmitidos, las condiciones del tratamiento de los datos personales, y el tiempo de conservación de los mismos.

- Solicitar se actualicen, incluyan, rectifiquen o modifiquen, o de ser el caso supriman o cancelen datos personales cuando estos sean parcial o totalmente inexactos, incompletos, cuando se ha advertido u omitido, error o falsedad, cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hayan sido recopilados o cuando hubieran vencido el plazo para su tratamiento.
- Siempre que por Ley, no se disponga lo contrario y cuando no hubiera prestado consentimiento, el titular de datos personales puede oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una situación personal. En caso de oposición justificada, el titular o el encargado del tratamiento de datos personales, según corresponda, debe proceder a su supresión conforme a Ley.

Para ejercer sus derechos los Usuarios podrán dirigirse a cualquier Agencia EREP-RENIEC. Para el ejercicio de tales derechos, el Usuario deberá identificarse a través de su documento de identidad vigente.

13. TRATAMIENTO DE LOS DATOS PERSONALES O DE LA INFORMACIÓN PROPORCIONADA POR LOS USUARIOS

Sin perjuicio de sus facultades legales, el RENIEC en su rol como ECERNEP, ECEP-RENIEC y EREP-RENIEC, sólo efectúa tratamiento de aquellos datos personales o información que han sido entregados voluntariamente por los Usuarios en los respectivos trámites para la prestación del Servicio de Certificación Digital.

Los procesos de tratamiento de información (recolección, registro, organización, visualización, almacenamiento, procesamiento, conservación, elaboración, modificación, extracción, consulta, bloqueo, supresión, comunicación y uso de la información personal) tienen como propósito la adecuada gestión y control de los servicios contratados por el Usuario, así como también la visualización o envío por medios impresos y telemáticos de información concerniente al Servicio de Certificación Digital. Estos procesos de tratamiento incluyen, pero no se encuentran limitados a:

- Emisión, cancelación o revocación de oficio de Certificados Digitales.
- Actualización de la información personal del Usuario.
- Verificación del estado de cancelación o revocación de los Certificados Digitales en la CRL.

- Creación de un banco de datos personales para gestionar la información de manera efectiva y eficiente.
- Sistema de gestión de la ECERNEP, ECEP-RENIEC y las EREP-RENIEC.

14. TRANSFERENCIA DE DATOS PERSONALES

RENIEC en su rol de ECERNEP-RENIEC, ECEP-RENIEC y EREP-RENIEC, y, dentro del marco de la IOFE, así como, en atención al deber de colaboración entre entidades del sector público⁸, podrá transferir a otras entidades de la Administración Pública, los datos personales de los Usuarios.

La entidad receptora de los datos personales es responsable de garantizar la protección de los datos personales transferidos.

Conforme el Decreto Legislativo N° 1353 si con posterioridad al consentimiento se produce la transferencia de datos personales por fusión, adquisición de cartera, o supuestos similares, el nuevo titular del banco de datos debe establecer un mecanismo de información eficaz para el titular de los datos personales sobre dicho nuevo encargado de tratamiento.

Sin perjuicio de lo expuesto, el Encargado de Tratamiento de Datos Personales⁹ deberá asegurarse de que toda transferencia de datos cuente con el consentimiento del titular de los datos personales, salvo excepciones previstas en la Ley y su Reglamento.

Toda transferencia de datos personales, tanto a nivel nacional como internacional procederá con autorización de cada encargado del banco de datos personales, y el medio por el cual se llevará a cabo dicha transferencia de datos deberá cumplir con la política de seguridad de la información vigente. En caso sea necesario efectuar un flujo transfronterizo de datos personales, los encargados de cada banco de datos deben garantizar que el proveedor destinatario mantenga los niveles de protección adecuados conforme a Ley vigente.

15. RESPONSABILIDAD DE LOS USUARIOS

El RENIEC asume que la información personal proporcionada por el Usuario es verídica; éste es responsable de comunicar a las EREP-RENIEC, y en cuanto sea aplicable a la ECERNEP, de manera inmediata, cualquier modificación en la misma. El Usuario asumirá las responsabilidades por los daños y perjuicios que pudiera causar por aportar datos falsos, incompletos o inexactos. En este caso, corresponderá al Usuario sufragar los costos que sean necesarios para la corrección y/o modificación de sus datos personales, el cual implica la emisión de un nuevo Certificado Digital. En caso los errores le fueran imputables a la EREP-RENIEC, no será necesario el pago de costo alguno.

16. DELIMITACIÓN DE RESPONSABILIDAD DEL RENIEC

El RENIEC está exento de toda responsabilidad cuando el error o la omisión de algún dato en su Certificado Digital devienen de la información consignada por el

⁸ Artículo 76 de la Ley N° 27444 – Ley del Procedimiento Administrativo General.

⁹ Conforme el artículo 2° de la Ley 29733, Ley de Protección de Datos Personales modificada por Decreto Legislativo 1353 “encargado de tratamiento de datos personales es la persona que realiza el tratamiento de datos personales por encargo del titular del banco de datos personales en virtud de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación” o tercerización.

Usuario o por un tercero en las solicitudes de emisión o cancelación del Certificado Digital.

Asimismo, el RENIEC no se hace responsable por cualquier violación a la confidencialidad que en el uso de sus datos personales pudieran incurrir los propios Usuarios.

17. CORRECCIÓN DE LA INFORMACIÓN PERSONAL

El Usuario que necesite actualizar o corregir la información personal contenida en su certificado digital, deberá solicitar inmediatamente a las EREP-RENIEC la cancelación del mismo y obtener uno nuevo. Ello debido a que su Certificado Digital contiene datos de identificación y es firmado digitalmente por la ECEP-RENIEC como parte del proceso respectivo.

En caso el Usuario sólo desee actualizar o corregir cualquier información personal de nuestros registros que no se encuentre en su Certificado Digital, podrá realizarlo personalmente en una agencia de la EREP-RENIEC.

18. CONSULTA A LA LISTA DE CERTIFICADOS CANCELADOS (CRL)

El Tercero que Confía o Tercer Usuario que desea confiar en un Certificado Digital emitido por el RENIEC, podrá verificar el estado del mismo consultando la CRL, la cual está disponible en la URL consignada en el mismo Certificado.

19. RESPONSABLE DEL TRATAMIENTO DE LOS DATOS PERSONALES

El RENIEC es el titular del banco de datos personales del Servicio de Certificación Digital. La ECERNEP, ECEP-RENIEC y las EREP-RENIEC son los responsables del tratamiento de los datos personales, el cual comprende: recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación, o interconexión de los datos personales.

El Oficial de Privacidad de Datos será la persona de contacto de la ECERNEP, la ECEP-RENIEC y las EREP-RENIEC en todos los asuntos relativos a la protección de los datos personales.

Si se tiene alguna pregunta relacionada con la Política de Privacidad, es posible ponerse en contacto con nosotros a través de nuestro sitio web o escribirnos a la dirección de correo electrónico: **identidaddigital@reniec.gob.pe**

El RENIEC, en su rol de ECERNEP, ECEP-RENIEC y EREP-RENIEC, se reserva el derecho de modificar la presente POLÍTICA DE PRIVACIDAD, a fin de adaptarla a nuevos requerimientos en materia de legislación, jurisprudencia, técnica o cualquier otro motivo, en la medida que le permita mejorar los servicios que ofrece. Por este motivo, aconsejamos revisar periódicamente la Política de Privacidad en el sitio web: <https://pki.reniec.gob.pe/repositorio/>