Política de privacidad y protección de datos personales

Datos del documento	
Código	DA-NF-001
Versión	1.0
Clasificación	PÚBLICO
Elaborado por:	Revisado y aprobado por:
Carlos Arturo Peña Gonzaga	Carlos Arturo Peña Gonzaga
Empresa: Novacert S.A.C.S	Empresa: Novacert S.A.C.S
Fecha: 01/07/2026	Fecha: 01/07/2026

Contenido

HISTORIAL DE CAMBIOS 3
1. Objetivo 4
2. Obligaciones y recopilación de datos (principio de proporcionalidad) 4
2.1. Datos en Novafirma-APP 4
2.2. Finalidad del tratamiento 4
2.3. Trazabilidad y retención de datos 4
3. Garantías de privacidad y seguridad 4
4. Responsabilidades 5
4.1. Procedimiento para el ejercicio de derechos ARCO 5
5. Gestión de incidentes 6
6. Actualización 6
7. Glosario de términos 6
8. Referencias 7

HISTORIAL DE CAMBIOS			
Versión	**Fecha**	**Descripción del cambio**	**Autor**
1.0	01/07/2026	Creación inicial del documento	Carlos A. Peña Gonzaga

1. Objetivo

La presente política tiene por objetivo establecer los lineamientos técnico-jurídicos para el tratamiento de datos personales en los componentes del ecosistema **Novafirma** (SIGN, APP y SAS). **Novacert S.A.C.S.**, en su condición de **Prestador de Servicios de Certificación Digital** acreditado ante el **INDECOPI**, garantiza que el procesamiento de la información se realice en estricto cumplimiento de la Ley N.º 29733 (Ley de Protección de Datos Personales), su Reglamento y el marco normativo de la Infraestructura Oficial de Firma Electrónica (IOFE). La entidad reafirma su compromiso con la transparencia, la seguridad de la información y el derecho fundamental a la autodeterminación informativa de los usuarios.

2. Obligaciones y recopilación de datos (principio de proporcionalidad)

El tratamiento de datos personales se rige por el principio de proporcionalidad, limitando la recopilación a la información técnica y legal estrictamente necesaria para asegurar la validez jurídica de los actos electrónicos por equivalencia funcional.

2.1. Datos que recolectamos y en que aplicaciones

Siguiendo el principio de proporcionalidad, solo pedimos la información mínima necesaria para la correcta vinculación de tu identidad con tu certificado digital:

- **Novafirma-APP (Móvil):** Es el único componente de nuestro ecosistema que recolecta y almacena tu correo electrónico y número de DNI. Estos datos son obligatorios para vincular tu identidad digital a tu certificado digital. También puedes elegir darnos tu nombre y teléfono (opcional).

- **Novafirma-SIGN y Novafirma-SAS:** Estas aplicaciones no recopilan ni almacenan datos. Funcionan procesando los documentos de forma técnica sin guardar tus datos personales de acceso.

2.2. Finalidad del tratamiento

Los datos recabados son tratados exclusivamente para los siguientes fines:

- Identificación y relación con los certificados digitales a utilizar en la aplicación.
- Garantía de trazabilidad en las operaciones de firma digital.

2.3. Trazabilidad y retención de datos

Con fines de auditoría y conforme a las exigencias de la IOFE, el sistema registra de forma automática la fecha, hora y tipo de operación realizada.

3. Garantías de privacidad y seguridad

Novacert S.A.C.S. implementa medidas técnicas y organizativas de alto nivel para proteger la integridad de los datos:

- **No almacenamiento de claves privadas:** Se declara taxativamente que Novafirma nunca almacena, copia, accede ni transmite la clave privada ni el PIN del usuario. El software invoca exclusivamente el proveedor criptográfico del dispositivo o sistema operativo.
- **Gestión diferenciada de documentos:** En cumplimiento del principio de transparencia, se informa que los componentes **Novafirma-SIGN, Novafirma-SAS** y la versión gratuita de **Novafirma-APP** no almacenan los documentos firmados. No obstante, los usuarios de **Novafirma-APP Premium** cuentan con un repositorio seguro donde los documentos se almacenan para su gestión personal.
- **Exclusión de datos sensibles:** No se recopila información que revele origen étnico, opiniones políticas, convicciones religiosas, salud o vida sexual, conforme a la prohibición establecida en la Ley N.º 29733.
- **Detección de entornos modificados: Novafirma-APP** incorpora mecanismos que impiden el uso en dispositivos con privilegios de superusuario (root) o modo desarrollador activo, a fin de mitigar riesgos de suplantación o alteración del proceso de firma.
- **Confidencialidad:** Se aplican medidas técnicas y acuerdos de confidencialidad con el personal para evitar la alteración, pérdida o acceso no autorizado.

4. Responsabilidades

La gestión de la privacidad es una responsabilidad compartida entre el titular del banco de datos y el usuario:

Responsable	Obligación
Novacert S.A.C.S	Asegurar la integridad del software; realizar el tratamiento según la Ley N.º 29733 y atender derechos ARCO.
Usuario final	Garantizar la veracidad de los datos; custodiar con diligencia su clave privada y PIN; y operar el software en dispositivos en estado seguro, sin privilegios de superusuario (root) o modo desarrollador activo.

4.1. Procedimiento para el ejercicio de derechos ARCO

Novacert S.A.C.S. garantiza el ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO) conforme a la Ley N.º 29733, El usuario puede gestionar su información y la cancelación de su cuenta bajo el siguiente esquema:

- **Autogestión y cierre de cuenta para usuarios básicos:** El usuario puede modificar o eliminar en tiempo real sus nombres y número de teléfono desde la interfaz de **Novafirma-APP**. Para el cierre de la cuenta, los usuarios disponen de un botón específico en la aplicación que, tras una confirmación de seguridad, procesará el cierre inmediato de su perfil.

- **Autogestión y cierre de cuenta para usuarios premium:** El usuario puede modificar o eliminar en tiempo real sus nombres y número de teléfono desde la interfaz de **Novafirma-APP:** Los usuarios con suscripción premium cuentan con un repositorio seguro de documentos almacenados, al cierre

de la cuenta aceptarán el borrado permanente de estos documentos, este borrado es irreversible.

- **Gestión de credenciales de acceso:** Dado que el correo electrónico y el número de documento (DNIe) constituyen las credenciales de identidad y la puerta de acceso a la plataforma, cualquier solicitud de actualización del correo asociado al DNI deberá ser canalizada a través de soporte@novafirma.pe . El personal técnico de **Novacert S.A.C.S**. brindará la asistencia necesaria para asegurar la integridad de la cuenta del usuario.

- **Solicitud formal ARCO:** Para cualquier otro requerimiento que no se resuelva por los medios anteriores, el titular puede remitir una solicitud formal al correo de soporte@novafirma.pe , El personal técnico de **Novacert S.A.C.S**. brindará la asistencia necesaria en el detalle específico de su pedido.

5. Gestión de incidentes

Ante cualquier sospecha de vulneración de datos, el usuario debe actuar bajo el siguiente protocolo:

- **Reporte Inmediato:** Comunicación al correo soporte@novafirma.pe.
- **Plazo de Respuesta:** Novacert S.A.C.S. brindará una respuesta técnica o iniciará acciones de mitigación en un máximo de 72 horas hábiles.

6. Actualización

La presente política será objeto de revisión anual o extraordinaria ante modificaciones en la Ley N.º 29733.

7. Glosario de términos

- **Autenticación:** Proceso técnico que permite determinar y verificar la identidad de la persona que firma digitalmente un documento electrónico. Garantiza que el firmante es efectivamente quien dice ser, en función del certificado digital y la firma incrustada, aunque no otorga fe pública ni certificación notarial.
- **Certificado digital:** Documento electrónico generado y firmado digitalmente por una Entidad de Certificación. Contiene los datos que vinculan un par de claves (pública y privada) con la identidad de una persona natural o jurídica, confirmando su autenticidad.
- **CRL – Lista de certificados digitales revocados:** Relación en la que se incorporan los certificados digitales que han sido revocados por la Entidad de Certificación, de acuerdo con lo establecido en el Reglamento de la Ley de Firmas y Certificados Digitales. Permite verificar que un certificado ya no es válido.
- **Documento Nacional de Identidad Electrónico (DNIe):** Credencial de identidad digital emitida por el **RENIEC**. Permite acreditar la identidad de las personas tanto de manera presencial como no presencial y contiene certificados digitales que habilitan al ciudadano a firmar documentos electrónicos con validez legal.
- **Equivalencia funcional:** Principio jurídico según el cual los actos realizados por medios electrónicos que cumplen con las disposiciones legales vigentes poseen la misma validez

y eficacia que los realizados en soporte físico o convencional, pudiendo sustituirlos para todos los efectos legales.

- **Firma digital:** Firma electrónica que utiliza técnicas de **criptografía asimétrica**, basada en un par de claves único (clave privada y clave pública) relacionadas matemáticamente. Garantiza la **autenticidad, integridad y no repudio** del documento electrónico.
- **Identidad:** Atributo que permite reconocer y distinguir a una persona natural o jurídica en el entorno digital, mediante el uso de certificados digitales y credenciales electrónicas reconocidas por la Infraestructura Oficial de Firma Electrónica.
- **Infraestructura Oficial de Firma Electrónica (IOFE):** Sistema confiable, acreditado, regulado y supervisado por la Autoridad Administrativa Competente (INDECOPI). Está conformado por las Entidades de Certificación, Entidades de Registro o Verificación, la Entidad de Certificación Nacional para el Estado Peruano, y los Prestadores de Servicios de Valor Añadido. Su finalidad es garantizar la integridad de los documentos electrónicos y la identidad de su autor.
- **Integridad:** Propiedad que asegura que la información contenida en un documento electrónico no ha sido alterada ni modificada desde su generación, transmisión o almacenamiento, salvo lo autorizado por su emisor.
- **TSL (Trust-service Status List):** Listado oficial que contiene los nombres y certificados de las Entidades Prestadoras de Servicios de Certificación consideradas confiables por la Autoridad Administrativa Competente. En el Perú, es gestionada y firmada por **INDECOPI** a efectos de asegurar la confianza en los servicios digitales.

8. Referencias

- Ley de Protección de Datos Personales Nº 29733.
- Decreto supremo Nº 003-2013-JUS, Reglamento de la Ley Nº 29733
- Ley de Firmas y Certificados Digital Nº 27269.
- Decreto Supremo Nº 052-2008-PCM, Reglamento de la ley Nº 27269.
- Decreto Supremo Nº 026-2016-PCM, 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
- INDECOPI – Guía de acreditación de aplicaciones de software de firma electrónica (Anexo A), Versión 4.0 (o versión vigente).
- Decreto Legislativo Nº 1412, Ley de Gobierno Digital.
- Términos y condiciones de uso – Novafirma