PLAN DE PRIVACIDAD

IDENTITY DEL PERÚ S.A.

RUC Nº 20607123463

Versión 1.1 de 15 de julio de 2025.

Clasificación: Público

Elaborado por:	Eduardo Nascimento de Oliveira Supervisor de Compliance
Aprobado por:	Ing. Augusto Castañeda Chávez Responsable de la EC
Dirigido a:	Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI)
Tipo de Documento:	Plan de Privacidad
Versión:	1.1
Fecha de elaboración:	30/05/2025

ÍNDICE

PLAN DE PRIVACIDAD DE LA ENTIDAD DE CERTIFICACIÓN DE IDENTITY DEL PERU S.A.

1. INTRODUCCIÓN

IDENTITY DEL PERÚ S.A. es una empresa privada reconocida en el mercado nacional que brinda el servicio de Identidad Digital, Comunicaciones Seguras, Venta Licencias de Certificados Digitales y Tecnologías de Firmas Electrónicas (Simples, Avanzadas y Cualificadas).

IDENTITY DEL PERÚ S.A. presenta y declara este documento como su PLAN DE PRIVACIDAD aplicado a su ENTIDAD DE CERTIFICACION en lineamiento a su DPC/CPS en el marco de la Infraestructura Oficial de Firma Electrónica (IOFE) regulado por INDECOPI.

2. PARTICIPANTES

2.1. **EC - IDENTITY DEL PERÚ S.A.** (Autoridad o Entidad de Certificación Digital, en proceso de Acreditación como PSC EC en la IOFE-INDECOPI), que a su vez es una sociedad peruana que pertenece al Grupo Soluti.

2.2. **ER – IDENTITY DEL PERÚ S.A.** empresa que presta los servicios de registro o verificación, tanto de personas naturales como jurídicas, a nivel nacional en la República del Perú, conforme a lo establecido en la Declaración de Prácticas Entidad de Registro (https://soluti.pe/legal/er). Esta sociedad se encuentra actualmente acreditada como Entidad de Registro (ER) según Resolución Nº 269-2024/DGI-INDECOPI emitido por la IOFE-INDECOPI.

2.3. La **EC y ER de IDENTITY DEL PERÚ S.A.** han celebrado un Acuerdo de Vinculación para brindar el servicio de registro y emisión de certificados digitales, por intermedio de un(a) operador(a) de registro[1] capacitado(a) para esta función. A través de este acuerdo de vinculación se gestionarán la aprobación de las solicitudes de los servicios de certificación digital, por lo que la responsabilidad de la disponibilidad y seguridad de estos sistemas depende de ésta última. La ER – IDENTITY DEL PERÚ S.A. brinda el servicio de venta de certificados digitales emitidos por EC – IDENTITY DEL PERÚ S.A., a través de su plataforma virtual[2], a la cual los solicitantes pueden acceder a través del siguiente enlace web: https://certificacion.soluti.pe/. Las comunicaciones entre la ER y EC se realizan vía web/online de manera ininterrumpida, según los niveles de disponibilidad y recuperación brindados y declarados por cada EC. La ER tiene procedimientos de contingencia para acceder a los sistemas en casos de corte del servicio de Internet. La disponibilidad del servicio web de registro es provisto por cada EC y es responsabilidad de IDENTITY DEL PERÚ S.A el mecanismo de contingencia utilizado Mediante esta plataforma virtual interna, GRAMD llevará un registro de los datos de cada Titular y/o Suscriptor de un certificado digital. La responsabilidad de la disponibilidad y seguridad de este sistema depende de GRAMD.

2.4. **Suscriptor o titular del certificado digital:** Es la persona natural responsable de la generación y uso de la clave privada, a quién se le vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando su clave privada. En el caso que el titular del certificado digital sea una persona natural, sobre ella recaerá la responsabilidad de suscriptor. En el caso que una persona jurídica sea el titular de un certificado digital, la responsabilidad de suscriptor recaerá sobre el representante legal designado por esta entidad. Si el certificado está designado para ser usado por un agente automatizado, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderán a la persona jurídica, la cual debe ser dueña del agente automatizado. La atribución de responsabilidad de suscriptor, para tales efectos, corresponde a la misma persona jurídica.

- **Titular de Certificado Digital:** Persona natural o jurídica a quien se le atribuye de manera exclusiva un certificado digital. La EC IDENTITY DEL PERÚ S.A., brinda servicios de certificación digital únicamente a personas naturales o jurídicas bien identificadas por la ER IDENTITY DEL PERÚ S.A. y otras ER acreditadas en la IOFE que procedan a vincularse.
- **Tercero que confía o tercer usuario:** Se refiere 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.

[1] Trabajador(a) de IDENTITY DEL PERÚ S.A.
[2] Plataforma Online llamada Centro de Certificación Digital (CCD) de Soluti.

3. DEFINICIONES Y ABREVIACIONES

Entidad de Certificación (EC):	Persona jurídica 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.
Entidad de Registro o Verificación (ER):	Persona jurídica, con excepción de los notarios públicos, encargada del levantamiento de datos, comprobación de estos respecto a un solicitante de un mecanismo de firma electrónica o certificación digital, la aceptación y autorización de las solicitudes para la emisión de un mecanismo de firma electrónica o certificados digitales, así como de la aceptación y autorización de las solicitudes de cancelación de mecanismos de firma electrónica o certificados digitales. Las personas encargadas de ejercer la citada función serán supervisadas y reguladas por la normatividad vigente.

Declaración de Prácticas de Certificación Digital (CPS):	Documento oficialmente presentado por una Entidad de Certificación a la Autoridad Administrativa Competente, mediante el cual define sus Prácticas de Certificación.
Operador de Registro de Datos:	Persona responsable de representar a la Entidad de Registro en las actividades de registro, recepción, validación y procesamiento de solicitudes.
Prácticas de Certificación:	Son las prácticas que establecen las actividades y requerimientos vinculados a la emisión de cada certificado digital.

4. INFORMACIÓN DE CONTACTO

La persona responsable de la administración y ejecución del presente PLAN DE PRIVACIDAD es ubicable mediante la siguiente información de contacto:

- Nombres: NASCIMENTO DE OLIVEIRA, EDUARDO
- Cargo: SUPERVISOR DE COMPLIANCE
- E-mail: privacidad@solutitech.com
- Teléfono: +51 (01) 5105161
- Dirección Legal: Calle Las Orquídeas 585, Oficina 1207, San Isidro, Lima-Perú

5. ALCANCE

El presente plan es de cumplimiento obligatorio para el personal de la EC de IDENTITY DEL PERÚ S.A. y personas que participan de las operaciones críticas de los servicios de emisión de certificados digitales.

6. INFORMACION RECOPILADA Y PROTEGIDA

Como parte de las operaciones de emisión de Certificados Digitales, en su calidad de EC, IDENTITY DEL PERÚ S.A., recopila la siguiente información de los suscriptores y/o titulares de certificados digitales:

- Nombres y Apellidos completos, Número de Identificación y Documento de identidad personal, además de direcciones declaradas en los documentos de identidad.
- Datos biométricos de identificación personal, incluyendo la fotografía que aparece en su documento de identidad.
- Documentación legal; como Vigencias de Poder de representantes legales, Copias Literales de personas jurídicas, y Ficha R.U.C. tanto de empresas u organizaciones, y personas naturales.
- Contratos de solicitud de servicios.

7. TRATAMIENTO DE LOS DATOS PERSONALES

Se considera como información no privada, la siguiente:

- Información del suscritor que se encuentre públicamente disponible. En estos casos no será requerida autorización del usuario para dar publicidad a esta información.

Deberá considerarse como información de identificación personal, la siguiente:

- Datos e información conforme a lo establecido por la Ley de Protección de Datos Personales Ley N.° 29733. Se considera información personal, cualquier información relativa a un individuo identificado o identificable.
- Información que pueda permitir la construcción de un perfil de las actividades de los usuarios de los servicios de certificación.
- En todos los casos, figurará en el documento de “Política de Privacidad” que deberá ser aceptada por el Titular y/o Suscriptor de un certificado digital, su consentimiento para el tratamiento y almacenamiento de estos datos.

La información personal considerada como privada y de carácter personal, únicamente será divulgada en caso de que exista consentimiento expreso previo y por escrito, firmado para tales efectos por el titular de dicha información o medie una orden judicial o administrativa que así lo determine.

Asimismo, es preciso señalar respecto al tratamiento de datos personales, que el Suscriptor y/o Titular de un certificado digital, podrá acceder a la página web: https://souti.pe/legal/privacidad y verificar la Resolución Nº 3694-2021-JUS/DGTAIPD-DPDP, emitido por el Ministerio de Justicia, mediante la cual se publica la Inscripción en el Registro Nacional de Protección de Datos Personales de IDENTITY DEL PERÚ S.A., de conformidad con lo dispuesto por la Ley N° 29733, Ley de Protección de Datos Personales.

8. FLUJO TRANSFRONTERIZO DE DATOS PERSONALES

Los contratos de los Titulares y/o Suscriptores de certificados digitales, contendrán cláusulas que soliciten el consentimiento de éstos para transferir los datos personales contenidos en estos documentos electrónicos, a la República Federativa de Brasil, y los Estados Unidos de América, países donde se encuentran las bases de datos de la Infraestructura de Clave Pública (PKI) de IDENTITY DEL PERÚ S.A..

9. IMPLEMENTACIÓN DE LOS PRINCIPIOS DE PRIVACIDAD

El presente Plan de Privacidad adopta lo establecido por el APEC a través de la Norma Marco sobre Privacidad y la Ley N° 29733, Ley de Protección de Datos Personales respecto de los principios que deben ser observados siempre que se realice algún tipo de labor o función que involucre la recolección, posesión, procesamiento, uso, transferencia o revelación de información personal.

9.1 MEDIDAS PREVENTIVAS

- Se restringirá el acceso a los datos personales a los Operadores de Registro de las EC vinculadas a la EC IDENTITY DEL PERÚ S.A.
- Estos datos serán protegidos contra acceso no autorizado.
- Se concientizará a todo el personal para no divulgar o exponer de manera accidental datos personales de los Titulares y/o Suscriptores de certificados digitales.
- Se implementarán procedimientos para documentar las prácticas en lo que respecta a la información personal que se recolecta durante las actividades de operación o comercialización de certificados digitales, las mismas que deben informar sobre:
  - El hecho de que se está recolectando información personal.
  - Los propósitos para los cuales se recolecta dicha información personal.
  - Los tipos de personas u organizaciones a las que dicha información podría ser revelada.
  - La identidad y ubicación del responsable de la información personal, Incluyendo información respecto a la forma de contactarlo en razón a sus prácticas y manejo de la información personal.
  - Las opciones y medios que ofrece el responsable de la información personal a los individuos para limitar el uso y revelación, así como los mecanismos para el acceso y corrección de su información.
  - Deberán tomarse todos los pasos razonablemente necesarios, a fin de asegurar que se provee tal información, sea antes o en el mismo momento en que se está efectuando la recolección de la información personal. Caso contrario, deberá proveerse esta información tan pronto como sea factible.

9.2 LIMITACIONES A LA RECOPILACIÓN

La recopilación de información personal debe encontrarse limitada a la información que es relevante para el propósito de la provisión y emisión de certificados digitales según la regulación local, y ésta información deberá ser obtenida de manera legal y apropiada, y con la debida información o consentimiento de la persona a la cual pertenece.

9.3 USO DE LA INFORMACIÓN PERSONAL

La información personal recopilada será usada en estricto cumplimiento de los propósitos de la recopilación o aspectos relativos a los mismos, a excepción:

- Que exista el consentimiento de la persona a la que pertenece la información persona recolectada.
- Que ésta información fuera necesaria para la provisión de un servicio o producto solicitado por dicha persona.
- Que la recopilación fuera permitida por mandato de Ley u otros instrumentos legales o exista algún tipo de pronunciamiento con efectos legales que lo autorizara.

9.4 ELECCIÓN

Cuando sea apropiado, se proveerá a los clientes y usuarios mecanismos claros, prominentes, fáciles de entender, accesibles y económicos a fin que puedan decidir respecto a la recopilación, uso y revelación de su información personal. Puede no resultar necesario que los responsables de la información provean estos mecanismos en los casos de recopilación de información que sea públicamente disponible.

9.5 INTEGRIDAD DE LA INFORMACIÓN PERSONAL

La información personal deberá ser exacta, completa y mantenerse actualizada en el extremo que fuere necesario para los propósitos de su empleo.

9.6 MECANISMOS DE SEGURIDAD

Los responsables de la información personal deberán protegerla, a través de mecanismos de seguridad apropiados contra riesgos tales como pérdida de la información o acceso indebido a la misma, así como contra la destrucción, uso, modificación o revelación no autorizada o cualquier otra circunstancia. Estos mecanismos deberán ser proporcionales a la naturaleza y gravedad del daño potencial, la sensibilidad de la información y el contexto en que ésta es mantenida, y deberán ser sometidas a revisiones periódicas.

9.7 ACCESO Y CORRECIÓN

Los Titulares y/o Suscriptores de certificados digitales, tendrán las facilidades de:

9.7.1. Obtener del responsable de privacidad de IDENTITY DEL PERÚ S.A, la confirmación respecto a si mantiene o no información personal que les concierne.
9.7.2. Comunicar su información personal, luego de haber probado suficientemente su identidad, dentro de un periodo de tiempo razonable; por una tarifa, si es que la hubiera, la cual no debe ser excesiva; de una manera razonable; de un formato que sea razonablemente comprensible.
9.7.3. Cuestionar la exactitud de la información que les concierne y de ser posible y apropiado, hacer que la información sea rectificada, completada, enmendada o borrada.
Deberá proveerse acceso y oportunidad para la corrección de la información, salvo cuando

- La carga o costo de hacerlo sea indebido o desproporcional a los riesgos de la privacidad individual en el caso en cuestión.
- La información no pueda ser divulgada por razones legales o de seguridad o para proteger información comercial de carácter confidencial.
- Se podría violar la privacidad de la información de personas diferentes al cliente.

Si una solicitud bajo el supuesto (9.1) o (9.2) o un cuestionamiento bajo el supuesto (9.3) es denegada, se debe informar al cliente las razones en las que se basa dicha denegatoria, así como también respecto a los mecanismos para cuestionar dicha decisión.

10. RESPONSABILIDADES

El Responsable de Privacidad (Supervisor de Compliance) gestiona la implementación y vela por el cumplimiento del presente Plan de Privacidad, así como de su revisión periódica, actualización, difusión y concientización y capacitación al personal y terceros para su adecuado cumplimiento.

11. PLAN DE AUDITORÍAS

11.1 AUDITORÍA DEL SERVICIO PARA EL PROVEEDOR DE INFRAESTRUCTURA

N°	Actividad	Responsable
	INICIO	
1	Anualmente, coordinar una sesión de auditoría con el Responsable del Servicio de Infraestructura y Alojamiento de Datos.	Ing. Augusto Castañeda Responsable de la EC
2	Revisar el informe anterior de auditoría	
3	Elaborar una lista de verificación de los controles que serán considerados, conforme a la Declaración de Prácticas y la política de Seguridad y cualquier cambio efectuado en la asignación de responsabilidades a	
4	Coordinar las fechas de auditoría	
5	Ejecutar la auditoría y emitir el informe correspondiente	
	FIN	

11.2. AUDITORÍAS INTERNAS DE PROCEDIMIENTOS

La EC realiza auditorías internas trimestralmente. El Responsable de la EC y El Gerente de Seguridad Digital y PKI se asegurarán de que se mantienen los siguientes controles:

- Seguridad física: controles de acceso, medidas de defensa civil, etc.
- Personal: Cambios o rotación en el personal, bajade operadores de registro, cambios en el organigrama de la EC y la ER.
- Documentos: Modificaciones en el procedimiento de verificaciones y registro, creacion de manuales o instrucciones técnicas, etc.

N°	Actividad	Responsable
INICIO		
1	Anualmente, específicamente en el primer semestre del año. Coordinar una sesión de auditoría con el Responsable de la ER de	Eduardo Nascimento de Oliveira Supervisor de Compliance
2	Revisar el informe anterior de auditoría	
3	Elaborar una lista de verificación de los controles que serán considerados, conforme a la Declaración de Prácticas y la política de Seguridad y cualquier cambio efectuado en la asignación de responsabilidades	
4	Coordinar las fechas de auditoría	Responsable de la EC
5	Ejecutar la auditoría y emitir el informe	Jefe de Tecnología

	correspondiente	
	FIN	

11.3. VERIFICACIONES INTERNAS

- La EC lleva a cabo verificaciones trimestralmente.
- El Supervisor de Compliance hace uso de los logs respecto a los siguientes temas:
  - Sistema de Registro, para validar que el OR instaló directamente los certificados en el repositorio del cliente y no en el repositorio de Windows de su propio computador.
  - Sistema Operativo del computador del OR.
  - Evidencias del flujo de procesos de emisión, renovación y revocación.
- El Supervisor y Coordinador de Seguridad de Información, luego de realizar la verificación, enviará un mensaje de correo electrónico al Gerente Oficial de Seguridad Digital y PKI indicando si se presentaron observaciones o si se realizó satisfactoriamente.

11.4. LINEAMENTOS DEL PROCEDIMIENTO

- El servicio brindado por la EC de IDENTITY DEL PERÚ S.A., deberá ser auditado respecto de las responsabilidades asignadas en la Declaración de Prácticas de Privacidad y la Política de Seguridad.
- El auditor asignado deberá ser verificado, respecto de sus antecedentes antes de tener acceso a los sistemas a auditar, asimismo deberá firmar el convenio de confidencialidad y la declaración jurada de libertad de conflictos de interés, asimismo, deberá acreditar tener el conocimiento y perfil especificado en el documento Roles de la ER.
- Las auditorías pueden ser trimestrales o al menos una vez al año y cada vez quelo requieran las autoridades administrativas competentes.

12. CONFORMIDAD

Este documento ha sido aprobado por el Responsable de EC IDENTITY DEL PERÚ S.A., y cualquier incumplimiento por parte de los trabajadores y terceros mencionados en el alcance de este documento, será comunicado a dicha autoridad para la ejecución de las correcciones pertinentes.