POLÍTICA Y PLAN DE PRIVACIDAD

Prestador de Servicios de Certificación Digital

Información del documento	
Nombre de documento: **Política y Plan de Privacidad de DIGILINK**	
Código de documento: **DL-POL-01**	
Versión: **1.1**	Aprobado por: **Responsable de la EC, ER y TSA**
Año: **2022**	Dirigido a: **INDECOPI**

Control de versiones		
Versión	**Fecha**	**Descripción**
1.0	27-11-2021	Elaboración de documento inicial.
1.1	22-03-2022	Se realizaron cambios en el formato.

ÍNDICE

1 INTRODUCCIÓN

DIGILINK S.AC., que en adelante llamaremos "DIGILINK", es una empresa peruana especializada en brindar servicios digitales innovadores de confianza basados en la firma digital desde el año 2021.

Entre sus servicios se encuentran sus funciones como Entidad de Certificación, Entidad de Registro y Autoridad de Sellado de Tiempo, para lo cual DIGILINK se encuentra acreditada ante el INDECOPI para su debido ejercicio.

En calidad de Entidad de Certificación, por medio de su proveedor de servicios GLOBALSIGN, emite certificados digitales a personas naturales y jurídicas.

Como Entidad de Registro, brinda los servicios de verificación de sus clientes, tanto para representantes legales, empleados o agentes automatizados, para la emisión, re-emisión o revocación de certificados digitales; así como el registro de las evidencias generadas.

Como entidad de Sellado de Tiempo, DIGILINK asume las responsabilidades de representación de los servicios de sello de tiempo brindados mediante su proveedor GLOBALSIGN, la cual es una infraestructura tercerizada y certificada.

2 OBJETIVO

Este documento tiene como objetivo la descripción de operaciones y prácticas de protección de datos personales que utiliza DIGILINK en calidad de Prestador de Servicios de Certificación, en el marco del cumplimiento de los requerimientos de las Guías de Acreditación establecidas por el INDECOPI.

3 OBJETO DE LA ACREDITACIÓN

El alcance de la acreditación cubre los sistemas de certificación digital que brinda DIGILINK en la entrega de sus servicios, y que son proporcionados por las EC, ER y TSA de DIGILINK.

4 DEFINICIONES Y ABREVIACIONES

Entidad de Certificación – EC	Entidad que presta servicios de emisión, revocación, re-emisión, modificación, suspensión de certificados digitales en el marco de la regulación establecida por la IOFE.
Entidad de Registro – ER	Entidad que realiza los procesos de verificación de identidad de los solicitantes de los servicios de

	certificación digital y que custodia de forma segura las evidencias de dichos procesos.
Autoridad de Sellado de Tiempo - TSA	Autoridad que emite los sellos de tiempo, en los cuales confían los suscriptores y terceros que confían.
Declaración de Prácticas de Certificación – DPC o CPS	Documento oficialmente presentado por una Entidad de Certificación a la Autoridad Administrativa Competente, mediante el cual define sus prácticas de certificación.
Política de Certificación – PC o CP	Conjunto de reglas que indican el marco de aplicabilidad de los servicios para una comunidad de usuarios definida y/o clase de aplicación con requisitos de seguridad comunes.
Titular	Entidad que requiere los servicios provistos por la EC de GlobalSign, y que está de acuerdo con los términos y condiciones de los servicios conforme a lo declarado en el presente documento.
Tercero que confía	Persona que recibe un documento, log, o notificación firmado digitalmente, y que confía en la validez de las transacciones realizadas.

5 RESPONSABILIDADES DE DIGILINK

Las responsabilidades contractuales, garantías financieras y coberturas de seguros de los servicios de certificación digital y de sellado de tiempo son brindadas por GLOBALSIGN, en calidad de proveedor de servicios de DIGILINK. Mientras que las responsabilidades contractuales, garantías financieras y coberturas de seguros de los servicios de validación y registro son brindadas directamente por DIGILINK.

DIGILINK representa todos los aspectos de ejecución de obligaciones contractuales, responsabilidad y mediación entre las personas jurídicas y naturales del Estado Peruano.

Las peticiones, quejas o reclamos para la atención de suscriptores y terceros debido a consultas relacionadas con el servicio que dispone la EC, ER y TSA, son recibidas directamente por DIGILINK mediante la línea telefónica o correo electrónico. Asimismo, pueden acercarse hacia la oficina de DIGILINK, indicando

que presenta una queja, reclamo o petición. Los datos de Contacto se encuentran en la sección 8 de la DPC.

6 ALCANCE

El presente documento es de cumplimiento obligatorio para el personal contratado por DIGILINK que participan de las operaciones críticas de los servicios de certificación descritos en sus documentos normativos.

En relación a los datos personales recogidos por DIGILINK, pero gestionados por GLOBALSIGN, se realiza de acuerdo a su política de privacidad publicada en su repositorio https://www.globalsign.com/en/repository

7 POLÍTICA DE PRIVACIDAD DE DATOS

DIGILINK garantiza la protección de datos personales de los suscriptores y titulares de los servicios de registro, en cumplimiento de la Ley de Protección de Datos Personales – Ley N°29733, la Norma Marco de Privacidad y la Guía de Acreditación de Entidades de Certificación Digital (EC), Entidades de Registro (ER) y de Servicios de Valor Añadido (SVA) tipo Autoridad de Sellado de Tiempo, en los ámbitos legales, regulatorios y contractuales.

Serán considerados como datos personales, la información de nombres completos, dirección física, correo electrónico y toda información que pueda vincularse a la identidad de una persona natural o jurídica, contenidos en los resultados de bases de datos, contratos y solicitudes de los suscriptores y titulares. Esta información será considerada como confidencial y será de uso exclusivo para las operaciones de registro, a excepción que exista un previo consentimiento del titular de dichos datos o medie una orden judicial o administrativa que así lo determine.

Es responsabilidad de los suscriptores garantizar que la información provista a la ER sea veraz y vigente. Asimismo, son responsables del perjuicio que pudieran causar por aportar datos falsos, incompletos o inexactos.

7.1 INFORMACIÓN RECOLECTADA Y PROTEGIDA

Como parte de las operaciones de certificación y registro, DIGILINK recolecta información de los suscriptores y titulares del siguiente tipo:

- Datos de identificación personal, tales como: nombres completos, dirección de correo electrónico, número de celular, domicilio y los resultados obtenidos de la base de datos del RENIEC, incluyendo la fotografía que aparece en su documento de identidad.

- Contrato de suscriptor/titular firmados.

7.2 TRATAMIENTO DE LOS DATOS PERSONALES

Con respecto al tratamiento de datos personales gestionados por DIGILINK, deberá considerarse como información no privada, la siguiente:

- Información personal públicamente disponible

En estos casos no será requerida autorización del usuario para dar publicidad a esta información.

Deberá considerarse como información privada, la siguiente:

- De conformidad con lo establecido por la Norma Marco sobre privacidad del APEC, se considera información personal, cualquier información relativa a un individuo identificado o identificable.
- Material comercialmente reservado de los PSC, de los suscriptores de la empresa y de los terceros que confían, incluyendo términos contractuales, planes de negocio y propiedad intelectual.
- Información que puede permitir a partes no autorizadas establecer la existencia o naturaleza de las relaciones entre los suscriptores, titulares y los terceros que confían.
- Información que pueda permitir a partes no autorizadas la construcción de un perfil de las actividades de los suscriptores, titulares o terceros que confían.
- Se debe asegurar la reserva de toda información que mantiene, la cual pudiera perjudicar la normal realización de sus operaciones.
- En todos los casos, figurará en la Política de Privacidad que deberá ser suscrita por el mismo, su consentimiento para el tratamiento y almacenamiento de estos datos.

La información personal considerada como privada únicamente será divulgada en caso que exista consentimiento 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.

Cualquier violación a la privacidad de esta información por parte del personal de DIGILINK o de los terceros subcontratados, será sujeto de sanción.

7.3 IMPLEMENTACIÓN DE LOS PRINCIPIOS DE PRIVACIDAD

El presente documento adopta lo establecido por el APEC a través de la Norma Marco sobre Privacidad 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.

7.3.1 MEDIDAS PREVENTIVAS

a) Se restringirá el acceso a los datos personales a personal autorizado.
b) Estos datos serán protegidos contra acceso no autorizado.
c) Se concientizará al personal para no divulgar o exponer de manera accidental datos personales de los usuarios.
d) Se implementarán procedimientos para documentar las prácticas en lo que respecta a la información personal que se recolecta durante las actividades de verificación y registro, las mismas que deben informar sobre:
   i. El hecho de que se está recolectando información personal;
   ii. Los propósitos para los cuales se recolecta dicha información personal;
   iii. Los tipos de personas u organizaciones a las que dicha información podría ser revelada;
   iv. 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;
   v. 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.
   vi. Deben 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.
e) Puede no resultar apropiado exigir que los responsables de la información personal provean información respecto a la recolección y uso de información que se encuentra públicamente disponible.

7.3.2 LIMITACIONES A LA RECOLECCIÓN

La recolección de información personal debe encontrarse limitada a la información que es relevante para el propósito para el cual se está recolectando y esta información deberá ser obtenida de manera legal y apropiada, y, en la medida de lo posible, con la debida información o consentimiento del individuo al cual pertenece.

7.3.3 USO DE LA INFORMACIÓN PERSONAL

La información personal recolectada será usada en estricto cumplimiento de los propósitos de la recolección o aspectos relativos a los mismos, excepto:

I. que exista consentimiento del individuo al que pertenece la información personal recolectada;

II. que esta información fuera necesaria para la provisión de un servicio o producto solicitado por el individuo; o
III. que la recolección fuera permitida por mandato de ley u otros instrumentos legales o exista algún tipo de pronunciamiento con efectos legales que lo autoriza.

7.3.4 ELECCIÓN

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

7.3.5 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.

7.3.6 SALVAGUARDAS A LA SEGURIDAD

Los responsables de la información personal deberán proteger la información personal que mantienen, a través de salvaguardas apropiadas 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 otro abuso. Estas salvaguardas 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 y reevaluaciones periódicas.

7.3.7 ACCESO Y CORRECCIÓN

Los individuos deben ser capaces de:

a) obtener del responsable de la información personal, la confirmación respecto a si mantiene o no información personal que les concierne.
b) 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; y
c) 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.

Debe proveerse acceso y oportunidad para la corrección de la información, salvo cuando:

I. La carga o costo de hacerlo sea indebido o desproporcionada a los riesgos de la privacidad individual en el caso en cuestión;
II. la información no pueda ser divulgada por razones legales o de seguridad o para proteger información comercial de carácter confidencial; o
III. se podría violar la privacidad de la información de personas diferentes al individuo.

Si una solicitud bajo el supuesto (a) o (b) es denegada, se debe informar al individuo las razones en las que se basa dicha denegatoria y se le debe informar respecto a los mecanismos para cuestionar dicha decisión.

8 RESPONSABLE DE SEGURIDAD Y PRIVACIDAD

El Responsable de Seguridad y Privacidad de DIGILINK gestiona la implementación y vela por el cumplimiento del presente documento así como de su revisión periódica, actualización, difusión y concientización y capacitación al personal y terceros para su adecuado cumplimiento.

9 CONFORMIDAD

Este documento ha sido aprobado por el Responsable de la EC, ER y TSA de DIGILINK, y cualquier incumplimiento por parte de los empleados, contratistas y terceros mencionados en el alcance de este documento, será comunicado a dicha autoridad para la ejecución de las sanciones respectivas.

Firmado por: JOSE ENRIQUE CAMARENA MEJIA
DNI:08083238
RUC:20606433507
Motivo: FIRMA DIGITAL