INDECOPI
Plan de Privacidad de ECERTLA S.A.C.

Norma(s) que Aplican	Refer.Normativa	Area Proceso	Código
INDECOPI - SID	ANEXO VI: PRIVACIDAD NORMA MARCO DE PRIVACIDAD	**SYC: Seguridad y Compliance** **CISEG: Ciberseguridad**	**PE-SYC-0001**
INDECOPI - ER	ANEXO VI: PRIVACIDAD NORMA MARCO DE PRIVACIDAD		

Nombre Aprobador	Fecha Creación	Fecha Aprobación	Fecha Vigencia	Revisión	Primera Revisión
Aquiles Moya	**18-01-2024**	**18-01-2024**	**18-01-2024**	**3**	**01-12-2023**

Propietario de la Información	Propietario del Proceso	Propietario de Sistema	Propietario del Riesgo	Clasificación de la Información
CISO	**CISO**	**Gerente General**	**Gerente Comercial**	**Uso Interno**

1. Introducción

ECERTLA S.A.C., que en adelante llamaremos “ECERT", es una empresa peruana fundada en el año 2023 con el objetivo de brindar servicios basados en soluciones digitales y firma digital, firma electrónica e identidad digital en latinoamérica.

Como parte de los servicios relacionados a la firma digital, ECERT es una Entidad de Registro, y un Prestador de Servicios de Valor Añadidos (SVA) acreditado ante el INDECOPI para su debido ejercicio.

En calidad de Entidad de Registro brinda los servicios de verificación de sus clientes, tanto para personas naturales, personas jurídicas, como paso previo a la emisión de certificados digitales.

ECERT brinda los servicios de firma digital a través de plataformas o de terceros que se interconectan al SID portal empresas. Entre los tipos de certificados digitales que se brindan para realizar las transacciones de firma se encuentran:

- Certificado Digital de Persona Natural para Persona Natural;
- Certificado Digital de Persona Jurídica para Representante Legal;
- Certificado Digital de Persona Jurídica de Pertenencia a Empresa (Conocido también como certificado de Atributo o certificado de Empleados o Certificados profesional colegiado);
- Certificado Digital de Persona Jurídica para Agente Automatizado.

Los certificados emitidos son provistos por la Entidad de Certificación de BIT4ID S.A.C., la cual forma parte de los Prestadores de Servicios de Certificación Digital acreditados por el INDECOPI.

En calidad de Prestador de Servicios de Valor Añadido – SVA como Sistema de Intermediación Digital "ECERT" provee la plataforma ***Portal Empresa***, la cual mantiene las funcionalidades necesarias para regular y controlar la gestión de usuarios y el intercambio seguro de información, así como la generación y protección de registros auditables de las transacciones realizadas. Para realizar esto de manera más segura y automatizada, Portal Empresas se conecta a los servicios de registro, y automatiza los procesos de recojo de evidencias y validación de identidad, utilizando para ello, herramientas de biometría facial interconectada con el servicio de Consulta en Línea del RENIEC.

2. Objeto

Este documento tiene como objetivo la descripción de operaciones y prácticas de protección de datos personales que utiliza ECERT en calidad de Entidad de Registro o Verificación y como Prestador de Servicios de Valor Añadido – SVA como Sistema de Intermediación Digital, en el marco del cumplimiento de los requerimientos de la "Guía de Acreditación de Entidades de Registro o Verificación (ER)" y la "Guía de Acreditación de Prestadores de Servicios de Valor Añadido SVA" establecida por el INDECOPI.

3. Objeto de acreditación

El objeto de la acreditación cubre los sistemas de registro que utiliza ECERT en la entrega de sus servicios, y que son proporcionados por las Entidad de Certificación de BIT4ID y al Sistema de Intermediación Digital de ECERT, los cuales utiliza procesos de firma digital para resguardar la autenticidad, integridad y confidencialidad de las transacciones.

4. Definiciones y abreviaciones

Certificación - EC: Entidad que presta servicios de emisión y revocación 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.

Política de Certificación: Conjunto de reglas que indican el marco de aplicabilidad de los servicios para una comunidad de usuarios definida.

Titular: Entidad que requiere los servicios provistos por las EC 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 firmada digitalmente y que confía en la validez de las transacciones realizadas.

PSVA - Prestador de Servicios de Valor Añadido: Entidad que presta servicios que implican el uso de firma digital en el marco de la regulación establecida por la IOFE.

SVA - Servicios de valor añadido: Servicios compuestos por tecnología y sistemas de gestión que utilizan certificados digitales garantizando la autenticidad e integridad de los mismos durante su aplicación.

5. PKI Participantes

5.1 Entidad de certificación BIT4ID

BIT4ID, en su papel de Entidad de Certificación acreditada, es una persona jurídica privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital.

5.2 Entidad de registro ECERT

ECERT brinda los servicios de Entidad de Registro la cual se encarga de certificar la validez de la información suministrada por el solicitante de un certificado digital mediante la verificación de su identidad y su registro.

5.3 Proveedor de servicios de certificación digital

Los proveedores de servicios de certificación son terceros que prestan su infraestructura o servicios tecnológicos a la Entidad de Registro de ECERT cuando esta entidad así lo requiere y garantizan la continuidad del servicio a los suscriptores y titulares durante todo el tiempo en que se hayan contratado los servicios de certificación digital.
Actualmente, los servicios de certificación digital que ofrece ECERT son provistos por la EC de BIT4ID.

5.4 Prestador de servicios de valor añadido - SID

ECERT, como PSVA, ofrece un Sistema de Intermediación Digital que actúa como plataforma para la firma de documentos electrónicos, mantiene los registros y disponibiliza los documentos firmados a través de dicha plataforma.

5.5 Titular

Titular es la persona natural o jurídica a cuyo nombre se expide un certificado digital y por tanto actúa como responsable del mismo confiando en él, con conocimiento y plena aceptación de los derechos y deberes establecidos y publicados en la RPS de ECERT.
La figura de Titular será diferente dependiendo de los distintos certificados emitidos por BIT4ID como prestadores de servicios de ECERT conforme a lo establecido en la Política de Certificación.

5.6 Suscriptor

Conforme a la IOFE el Suscriptor es el responsable del uso de la clave privada, a quien 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 atribución de responsabilidad de suscriptor, para tales efectos, corresponde a la misma persona jurídica.

5.7 Solicitante

Se entenderá por Solicitante, la persona natural o jurídica que solicita un Certificado emitido bajo la CPS de BIT4ID.
En el caso de los certificados de persona natural puede coincidir con la figura del Titular.

5.8 Tercero que confía

Tercero que confía son todas aquellas personas naturales o jurídicas que deciden aceptar y confiar en los certificados digitales emitidos por la Entidad de Certificación de BIT4ID. El Tercero que confía, a su vez puede ser o no titular.

5.9 Entidad a la cual se encuentra vinculado el titular

En su caso, la persona jurídica u organización a la que el Titular se encuentra estrechamente relacionado mediante la vinculación acreditada en el Certificado.

6. Responsabilidades

Las responsabilidades contractuales, garantías financieras y coberturas de seguros relacionados a los servicios de registro son brindadas por ECERT.
Asimismo, ECERT vela porque los servicios de registro o verificación se realicen conforme a la regulación vigente de la IOFE para realizar la verificación remota de identidad de las personas naturales y jurídicas solicitantes de los certificados digitales.

Las peticiones, quejas o reclamos para la atención de suscriptores y terceros debido a consultas relacionadas con el servicio que dispone la ER son recibidas directamente por ECERT mediante una línea telefónica o correo electrónico.

BIT4ID en calidad de EC es responsable de todos los aspectos de ejecución de obligaciones contractuales, responsabilidad y mediación entre las personas naturales y jurídicas del Estado Peruano relacionados a los servicios de emisión, confianza de la gestión del ciclo de vida de las claves de la CA, gestión del ciclo de vida de claves de certificados digitales, servicios de revocación de firmas digitales.
.

7. Alcance

El presente plan es de cumplimiento obligatorio para el personal contratado por ECERT que participan de las operaciones críticas de los servicios emitidos por ECERT descritos en sus Declaración de Prácticas de ER y SVA.

8. Plan de privacidad de datos

ECERT garantiza la protección de datos personales de los suscriptores y titulares de los servicios, 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 Registro o Verificación, la Guía de Acreditación de Prestadores de Servicio de Valor Añadido, en los ámbitos legales, regulatorios y contractuales.
Serán considerados como datos personales, la información de nombres, dirección, correo electrónico y toda información que pueda vincularse a la identidad de una persona natural o jurídica, contenidos en los 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.
Con este fin, se implementará un Plan de Privacidad con controles para la protección contra divulgación y uso no autorizado.
Es responsabilidad de los suscriptores garantizar que la información provista a ECERT sea veraz y vigente. Asimismo, son responsables del perjuicio que pudieran causar por aportar datos falsos, incompletos o inexactos.

8.1 Información recolectada y protegida

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

- Datos de identificación personal, incluyendo la fotografía que aparece en su documento de identidad.
- Contrato de solicitud de servicios.

8.2 Tratamiento de los datos personales

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 de 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 ECERT o de los terceros subcontratados, será sujeto de sanción.

8.3 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.

8.3.1 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.

8.3.2 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.

8.3.3 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 autorizará.

8.3.4 Elección

Cuando sea apropiado, se proveerá a los individuos mecanismos claros, prominentes, fáciles de entender, accesibles y económicos a fin de 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.

8.3.5 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.

8.3.6 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.

8.3.7 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 desproporcional 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 denegado 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.

9. Responsable de privacidad

El responsable de Seguridad y Privacidad de ECERT gestiona la implementación y vela por el cumplimiento del presente Plan, 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 privacidad de ECERT, 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.

10. De Gobierno

Respecto de esta Política las responsabilidades de los principales roles, son las que se describen a continuación:

10.1 Gerente General

a. Asegurar el establecimiento de esta Política, así como de su adecuación a los procesos de negocio.
b. Revisar al menos una vez al año esta Política, revisión que debe ser aprobada por el mismo Gerente General.

10.2 Comité del Sistema de Gestión

a. Asegurar la implementación de esta política, para lo cual le corresponde hacer seguimiento de la gestión de riesgos y oportunidades en cada sesión.
b. Informar al Gerente General y a la plana ejecutiva de los riesgos asociados a esta Política y su implementación, así como resolver respecto de las medidas de mitigación.

10.3 Propietario del proceso, del riesgo o del activo de la información

a. Asegurar la aplicación y seguimiento de esta Política y los documentos relacionados.
b. planificar sus procesos, objetivos e indicadores, de forma coherente con la presente Política, con la finalidad de minimizar los riesgos, gestionar las oportunidades, verificar el desempeño y optimizar los resultados de la organización en su conjunto.

11. Contexto Normativo

1. Guía de Acreditación de Prestadores de Servicio de Valor Añadido, INDECOPI
2. Ley de Firmas y Certificados Digitales – Ley 27269
3. Decreto Supremo 052-2008
4. Decreto Supremo 070-2011

12. Publicación

La Declaración de Prácticas de Registro y la Declaración de Prácticas de SVA de ECERT, la Política de seguridad, Política y Plan de Privacidad, y otra documentación relevante son publicados en la página web de ECERT:

https://ecert.ecertla.com/peru/

Todas las modificaciones relevantes serán comunicadas al INDECOPI y las nuevas versiones del documento serán publicadas en el mismo sitio web.
El presente documento es firmado por el Representante legal de ECERT antes de ser publicado, y se controlan las versiones del mismo, a fin de evitar modificaciones y suplantaciones no autorizadas.

13. Sencibilización y Capacitación

a. El Gerente General de ECERT reconoce como tareas prioritarias la sensibilización, capacitación y entrenamiento del personal, en materias de las indicadas en la presente Política.
b. Los ejecutivos de ECERT deben crear mecanismos para que esta política, las normas y sus procedimientos, sean conocidos y considerados permanentemente por todos los integrantes de la organización, asegurándose que los colaboradores asumen y comprenden sus responsabilidades. Estas acciones estarán contenidas en las actividades de capacitación anual al personal de ECERT.
c. Los ejecutivos de ECERT deben asegurar que todos los colaboradores cuenten con una inducción y sean capacitados en materias de esta política, manteniendo un canal de comunicación formal para informar a toda la organización respecto a los avances, logros y novedades en la materia, con el objetivo de crear una cultura de calidad dentro de la Organización.

14. Incumplimiento

a. Ante la ocurrencia de algún incumplimiento a las medidas orientadas a resguardar la presente política, el usuario que lo detecte debe informar a la brevedad a su jefatura directa y al Comité Sistema de Gestión, quienes analizarán el incumplimiento y deben gestionar las medidas necesarias para minimizar los potenciales daños a la empresa y lograr el cumplimiento integral de esta política, evitando que se reiteren situaciones similares.
b. Todo colaborador tiene la obligación de notificar cualquier actividad o situación que afecte o pueda afectar lo dispuesto en la presente Política. Dicha notificación se debe registrar conforme al Procedimiento Gestión de Incidentes (PR-SGI-0002).
c. Los incumplimientos graves, es decir, aquellos que afecten a los clientes y/o que manifiesten como quejas del cliente o de INDECOPI deben ser informados al Gerente General y al Directorio de ECERT.

15. Sanciones

a. Al colaborador que contravenga lo indicado en esta Política y/o los documentos relacionados a la misma, se le debe aplicar lo establecido en el Reglamento Interno de Orden, Higiene y Seguridad (RE-GER-0001), en cuanto a sanciones y multas.
b. Con relación al personal externo y/o proveedores que no cumplan con lo indicado en esta Política, dependiendo del tipo de incumplimiento se debe amonestar o rescindir el contrato.

16. Control de versiones

Control de versiones		
Versión	Fecha	Descripción
1.0	07-04-2023	Elaboración de documento inicial.
2.0	11-01-2024	- Se elimina la palabra "enrolados" se reemplaza por Persona natural, persona jurídica. - Se homologa el certificado profesional colegiado como persona jurídica, tal como lo tiene BIT4ID.

Fin del documento
Una copia impresa de este documento es válida sólo por el día en que se imprimió.
Cualquier modificación y/o copia total o parcial, por cualquier medio, queda totalmente PROHIBIDA.

Firmado digitalmente por:
IGOR VLADIMIR CONTRERAS
PLASENCIA DNI:08427612
RUC:20610663967
Motivo: Soy el autor del
documento
Fecha: 19/01/2024 15:21:01-0500