PRÁCTICAS DE CERTIFICACIÓN

Declaración de Prácticas del Servicio de Valor Añadido - SID

Norma(s) que Aplican	Referencia Normativa	Área Proceso	Código
ISO 9001:2015	8.2 Requisitos para los productos y servicios	GCOM: Gerencia Comercial	PC-GCOM-0003
INDECOPI - SID	3.2.11 Auditoría	PPKI: Gestión procesos de productos PKI (FES - FEA)	
INDECOPI - ER	3.2.8 Gestión de la seguridad		
ISO/IEC 27001:2022	4 Contexto de la organización		

Nombre Aprobador	Fecha Creación	Fecha Aprobación	Fecha Vigencia	Revisión	Primera Revisión
Alfredo Guardiola	19-02-2025	19-02-2025	20-02-2025	4	07-04-2023

Propietario de la Información	Propietario del Proceso	Propietario de Sistema	Propietario del Riesgo	Clasificación de la Información
Gerente de Cumplimiento y Consultoría	Responsable Sistema de Intermediación Digital	Gerente General	Responsable Sistema de Intermediación Digital	Público

Firma electrónica avanzada
ALFREDO JUAN GUARDIOLA CARRERE
2025.02.20 21:10:43 -0300

CONTENIDO

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 Empresas, la cual mantiene las funcionalidades necesarias para regular y controlar la gestión de usuarios y el intercambio seguro de información, la gestión de las bolsas de firmas contratadas, 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 OBJETIVO

Este documento tiene como objeto la descripción de las operaciones y prácticas que utiliza ECERT para la administración de sus servicios 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 Prestadores de Servicios de Valor Añadido SVA" establecida por el INDECOPI.

3 OBJETO DE LA ACREDITACIÓN

El alcance de la acreditación cubre al Sistema de Intermediación Digital de ECERT, los cuales utilizan procesos de firma digital para resguardar la autenticidad, integridad y confidencialidad de las transacciones.

ECERT tiene la obligación de exigir el cumplimiento de las directivas establecidas para sus proveedores, las mismas que están alineadas con la presente DPSVA. En ese sentido, es responsable ante sus clientes de la calidad y seguridad de los servicios brindados.

Los proveedores por sí mismos no se encuentran amparados por la presente acreditación, sino solamente a través del control de calidad y seguridad que exige ECERT a sus proveedores.

4 DEFINICIONES Y ABREVIACIONES

ER - Entidad de Registro: 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.

EC- Entidad de Certificación: Entidad que presta servicios de emisión y revocación de certificados digitales en el marco de la regulación establecida por la IOFE.

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.

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

INDECOPI: Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual: Es la Autoridad Nacional de Protección del Consumidor que fomenta en el mercado mejores decisiones de consumo, garantizando la protección de la salud y seguridad de los consumidores. Además de promover mecanismos para la prevención y solución de conflictos a nivel nacional.

CPS- Declaración de Prácticas de certificación: Declaración de los procedimientos y controles que adopta en cada etapa de los servicios y sistemas que brinda a sus clientes para la emisión de certificados digitales (BIT4ID).

RPS - Declaración de Prácticas de registro: Procedimientos y controles que se adopta en cada etapa de los servicios y sistemas que se brinda a los clientes de acuerdo con lo establecido por INDECOPI.

DPSVA - Declaración de Prácticas de Servicios de Valor Añadido: Procedimientos y controles que se adopta en cada etapa de los servicios y sistemas que se brinda a los clientes de acuerdo con lo establecido por INDECOPI.

SID - Sistema de Intermediación Digital: Plataforma de gestión necesario 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.

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.

Suscriptor: Entidad que requiere los servicios provistos por la SVA de ECERT 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.

IOFE- Infraestructura Oficial de Firma Electrónica: es el Sistema confiable, acreditado, regulado y supervisado por la Autoridad Administrativa Competente (INDECOPI).

SUNARP: Superintendencia Nacional de los Registros Públicos del Perú: Institución en Perú encargada de la administración y supervisión de los registros públicos, como el registro de propiedades, empresas y personas.

SUNAT: Superintendencia Nacional de Aduanas y de Administración Tributaria: Entidad peruana encargada de la administración y control de los impuestos, aduanas y tributos en el país.

RENIEC: Registro Nacional de Identificación y Estado Civil: Entidad encargada 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.

5 PARTICIPANTES DEL SVA

5.1 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.

5.2 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.

5.3 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 registro 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.

5.5 Comunidad de usuarios

Los servicios que provee ECERT como PSVA, podrán ser solicitados por personas naturales y por personas jurídicas tanto del sector privado como de la administración pública según lo indicado en la presente DPSVA.

5.6 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.

6 ALCANCE

La presente DPSVA, es de carácter público y se encuentra dirigida a todas las personas naturales y jurídicas, solicitantes, suscriptores, terceros que confían y público en general. La misma podrá ser consultada a través de la página web:

https://www.ecertla.com/peru/

7 RESPONSABILIDADES Y OBLIGACIONES

7.1 ECERT

Las responsabilidades contractuales, garantías financieras y coberturas de seguros son brindadas por ECERT.

ECERT es responsable de exigir y supervisar las operaciones de los servicios del Sistema de Intermediación Digital.

Las peticiones, quejas o reclamos para la atención de suscriptores y terceros debido a consultas relacionadas al servicio que dispone el Sistema de Intermediación Digital son recibidas directamente por ECERT mediante el siguiente correo electrónico mensajeria@ecert.pe o vía telefónica +51 1701 8614.

7.2 Usuarios

Los usuarios y solicitantes del Servicio de Valor Añadido provistos por ECERT, son responsables de revisar la presente DPSVA y las Políticas de SVA, a fin de ser enterados de las características de la plataforma de servicios, infraestructura y procedimientos empleados en la gestión de operaciones del Sistema de Intermediación Digital, así como las obligaciones de cada parte.

Es de exclusiva responsabilidad del usuario el almacenamiento de los documentos que procese a través del Sistema de Intermediación Digital, excluyendo de la responsabilidad de custodiar la información a ECERT.

7.3 Terceros que confían

Los terceros que confían del Servicio de Valor Añadido provistos por ECERT, deberán verificar la validez de los certificados digitales de los documentos o información procesada por los Sistemas de Intermediación Digital, así como tomar en cuenta cualquier limitación en el uso de los sistemas considerados en la DPSVA u otra precaución prescrita en los acuerdos.

7.4 Limitaciones de responsabilidad

ECERT no será responsable en ningún caso cuando se encuentre ante cualquiera de estas circunstancias:

1) Estado de Guerra, desastres naturales, funcionamiento defectuoso de los servicios eléctricos, las redes telemáticas y/o telefónicas o de los equipos informáticos utilizados por los usuarios o por los Terceros que confían, o cualquier otro caso de fuerza mayor.
2) Por el uso indebido del servicio.
3) En relación a acciones u omisiones del Suscriptor:
    a) Falta de veracidad de la información suministrada para solicitar el servicio.
    b) Negligencia en conservación de sus datos de acceso al servicio, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación.
    c) Extralimitación en el uso del servicio, según lo dispuesto en la normativa vigente y en la presente Declaración de Prácticas.
    d) Retraso en la comunicación de las causas de cancelación del servicio.

8 SISTEMA DE INTERMEDIACIÓN DIGITAL - PORTAL EMPRESA

El Sistema de Intermediación Digital de Portal Empresa es una solución digital que tiene la capacidad de gestión y firma de documentos electrónicos, mediante un proceso 100% online y con plena validez legal.

Portal Empresa nos permite la automatización de flujos de documentos integrado con firma electrónica.

Permite la creación y administración de documentos de todo tipo, los que pueden ser manejados por diferentes perfiles de usuario y con distintas atribuciones para cada uno de ellos.

Entre sus beneficios esta:

- Firma de documentos con firma digital y no repudio.
- Posibilidad de integración del cliente con Portal Empresa.
- Gestiona y envía documentos desde un solo lugar.
- Reduce el tiempo, utilizando flujos de firma predefinidos y gestionando contactos.

Asimismo, Portal Empresa es de acceso a nuestros clientes suscritos ingresando al siguiente link:

- https://portal.ecert.pe/Login

9 CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y OPERACIONALES

Los controles de seguridad abarcan el ambiente físico, las redes, los sistemas, entre otros; los cuales se especifican a continuación.

9.1 Control Físico

El acceso físico a ECERT dispone de un esquema de control de acceso. Asimismo, el acceso físico a la unidad que otorga los servicios del Sistema de Intermediación Digital será bajo estrictas normas de seguridad y monitoreo incluyendo esquemas electrónicos de identificación y control. Adicionalmente, este lugar dispone de elementos adecuados para la operación tales como aire acondicionado, sistema de detección y prevención de incendios, esquema seguro de respaldos externos para eventuales catástrofes.

9.2 Procedimiento de control

El control de las funciones se efectuará por medio de:

- Adecuada segregación de funciones.
- Control dual de las funciones de administración de los sistemas.
- Identificación y autenticación de cada rol.

9.3 Compromiso de seguridad y recuperación de desastres

9.3.1 Alta Disponibilidad

En el eventual escenario de no disponibilidad por la falla de una o más componentes, se evitarán las consecuencias negativas en el servicio mediante una configuración de alta disponibilidad, por medio de la duplicación de los servicios y equipos necesarios para otorgar los servicios críticos asociados al sistema de intermediación digital.

9.3.2 Soporte de desastres

Tratándose de un caso de desastre, para los sistemas críticos se dispone de un sitio alternativo remoto de procesamiento, para asumir las funciones, con indicación de los niveles de servicio y tiempo de recuperación comprometidos para continuar con los servicios de certificación de firma electrónica.

Para los servicios no críticos se dispone de un Plan de Contingencia probado que permite restablecer dichos servicios en un plazo adecuado a los tiempos involucrados con la emisión de Certificados.

Complementario a la solución de alta disponibilidad nuestro sistema de respaldo nos permite minimizar la pérdida de información.

Para asegurar la adecuada reposición de los servicios, en caso de fallas, se cuenta con Manuales que permitan superarla de manera estructurada.

9.4 Control de personal

9.4.1 Roles de confianza

ECERT declara que sus roles de confianza al cumplir son:

Gerente General: Responsable de liderar ECERT en su administración, gestión y control, velando por su rentabilidad y asegurando la continuidad operacional a todos sus clientes.

Responsable de Seguridad y Privacidad: Responsable general para aprobar, administrar y velar por el cumplimiento de las Políticas de Seguridad y la Privacidad de datos personales de los clientes.

Responsable del SID: Responsable de la dirección de las operaciones del SID conforme a la normativa vigente, para aprobar, revisar la implementación y cumplimiento de la Política y Declaración de Prácticas, la Política de Seguridad, la Política y Plan de Privacidad y todo documento normativo del SID.

Consultor: Responsable de la gestión del proyecto de implementación de los clientes B2B. Además de generar configuraciones en el Portal de Empresa para sus clientes persona natural, jurídica y operativos.

Responsable de Desarrollo: Responsable de asegurar los objetivos de la empresa a través de la planificación estratégica y dirección del desarrollo de software, cumpliendo plazos, costos, calidad y seguridad de la información.

Responsable de Mesa de servicios: Responsable de atender consultas y dar soporte de primer nivel a los clientes B2B.

Responsable de Operaciones TI: Responsable de asegurar los objetivos de la empresa a través de las operaciones TI y velar por la continuidad operacional asegurando el cumplimiento normativo.

9.4.2 Requerimiento de formación y retroalimentación

Como parte de las recomendaciones en que ECERT ha trabajado, se considera para el personal asociado, cursos de capacitación, los cuales en contenido, duración y fechas estimadas se encuentran descritos en el plan de capacitación anual. Este plan incluirá labores de re-entrenamiento de existir cambios tecnológicos, en las políticas o prácticas o cualquier documento que se considere relevante de ser informado.

9.4.3 Sanciones

El Reglamento Interno de Orden, Higiene y Seguridad considera las sanciones a las que se pueden ver expuestos las personas que laboran.

9.4.4 Requerimientos de contratación

Como parte de los requerimientos de contratación, todo trabajador de la Sistema de intermediación digital debe firmar un acuerdo de confidencialidad.

9.4.5 Documentación proporcionada al personal

ECERT pondrá a disposición de todo el personal que participa de los servicios de la SVA, la documentación donde se detallen las funciones encomendadas, las políticas y prácticas que rigen dichos procesos y la documentación de seguridad:

- Declaración de prácticas SVA
- Política de privacidad
- Plan de privacidad
- Política y Plan de seguridad del SVA

Adicionalmente se suministrará la documentación que precise el personal en cada momento, al objeto de que pueda desarrollar de forma competente sus funciones.

9.5 Generación del par de claves e instalación

Los datos de creación de firma asociados a los certificados siempre son generados por un mecanismo que se encuentra bajo el exclusivo control del suscriptor.

9.6 Protección de la clave privada

Respecto de la protección de los datos de creación de firma se debe considerar:

a) Protección del suscriptor: Los datos de creación de firma deben ser protegidos permanentemente por el suscriptor.

b) ECERT en ninguna circunstancia mantiene, custodia, protege o accede a los datos de creación de firma pertenecientes a un suscriptor.

9.7 Seguridad de redes

ECERT limita el acceso de sus redes al personal debidamente autorizado. Para lograr ello, se implementan controles para proteger la red interna de acceso por terceras partes, los datos sensibles son cifrados al momento ser intercambiado a través de redes no seguras y se garantiza que los componentes locales de red están ubicados en entornos seguros.

9.8 Seguridad Tecnológica

ECERT hace uso de procedimientos de pruebas y paso a producción de cualquier cambio que afecta al software del SID. Estos cambios están regulados por un procedimiento de control de cambio administrado por la Gerencia de Operaciones TI.

9.9 Procedimiento de Auditoría de seguridad

9.9.1 Tipos de eventos registrados

ECERT registra y guarda los logs de todos los eventos relativos al sistema de seguridad de la SVA. Estos incluyen los siguientes eventos:

- Encendido y apagado del sistema.

- Intentos de accesos no autorizados al sistema del SVA a través de la red.
- Intentos de accesos no autorizados a la red interna del SVA.
- Intentos de accesos no autorizados al sistema de archivos.
- Acceso físico a los logs.
- Cambios en la configuración y mantenimiento del sistema.
- Encendido y apagado de la aplicación del SVA.
- Intentos de creación, borrado, restablecimiento de contraseñas o cambio de privilegios.
- Intentos de inicio y fin de sesión.

Adicionalmente, ECERT conserva, ya sea manual o electrónicamente, la siguiente información:

- Registros de acceso físico.
- Mantenimiento y cambios de configuración del sistema.
- Altas y bajas de administradores del SVA.
- Informes de incidencias del servicio del SVA.

9.9.2 Frecuencia de procesado de los registros de auditoría

Se revisarán los logs de auditoría periódicamente y en todo caso cuando se produzca una alerta del sistema motivada por la existencia de algún incidente, en busca de actividad sospechosa o no habitual.

9.9.3 Periodo de conservación de los registros de auditoría

Se almacenará la información de los logs de auditoría por el tiempo que se considere necesario para garantizar la seguridad del sistema, de acuerdo a lo definido en el punto 9.9.1 de esta misma Declaración de prácticas.

9.9.4 Protección de los registros de auditoría

Los registros de auditoría se protegen mediante control de acceso. El personal de confianza de ECERT que accede a los log de auditoría solo tiene privilegios a la lectura de los registros.

9.9.5 Análisis de vulnerabilidades

El análisis de vulnerabilidades queda cubierto por los procesos de Auditoría de ECERTLA.

Anualmente se realizan los procesos de gestión de riesgos y vulnerabilidades dentro del marco de revisión de la regulación de INDECOPI.

10 PROTECCIÓN DE DATOS PERSONALES

ECERT garantiza la protección de datos personales de los clientes, en cumplimiento de la Ley de Protección de Datos Personales – Ley N°29733, la Norma Marco de Privacidad y la Guía de Acreditación de Servicios 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 clientes. Esta información será considerada como confidencial y será de uso exclusivo para las operaciones del servicio de valor añadido, 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.

11 PERSONA DE CONTACTO

Datos del Sistema de Intermediación Digital

- Nombre: María Valeska Flores
- Dirección Perú: Calle K n° 120, distrito de Miraflores, Provincia y Departamento de Lima, Perú.
- Dirección Chile: Monjitas 395, Piso 17, Santiago de Chile
- Teléfono Perú: +51 1701 8614
- Correo electrónico: mflores@ecertla.com
- Página Web: https://www.ecertla.com/peru/

12 ORGANIZACIÓN QUE ADMINISTRA LOS DOCUMENTOS

ECERT administra los documentos de Declaración de Prácticas, y todos los documentos normativos del SVA de ECERT.

Para cualquier consulta contactar:

- Nombre: Ignacio Vásquez
- Cargo: Responsable de Seguridad y Privacidad
- Dirección de correo electrónico: ivasquez@ecertla.com

13 PUBLICACIÓN DE LA DECLARACIÓN DE PRÁCTICAS

La Declaración de Prácticas - DPSVA de ECERT, así como la Política de Seguridad, Política y Plan de Privacidad del Servicio de Valor Añadido y otra documentación relevante son publicadas en la siguiente dirección:

- https://www.ecertla.com/peru/

Todas las modificaciones relevantes en la documentación de ECERT, serán comunicadas al INDECOPI y las nuevas versiones del documento serán publicadas en el mismo sitio web.

El presente documento es firmado por el responsable del Servicio de Valor Añadido de ECERT antes de ser publicado, y se controlan las versiones del mismo, a fin de evitar modificaciones y suplantaciones no autorizadas.

Las modificaciones relativas a la DPSVA u otra documentación relativa serán publicadas luego de ser informadas al INDECOPI.

13.1 Frecuencia de publicación

ECERT publica de forma inmediata en su página web: http://www.ecertla.com/peru/https://www.ecertla.com/peru/ cualquier modificación en la Declaración de Prácticas y/o Políticas, los cambios generados en cada nueva versión serán previamente informados al INDECOPI y esto se evaluará en las auditorías anuales de cumplimiento.

14 AUDITORÍAS

14.1 Frecuencia de Auditorías

Las auditorías internas se llevarán a cabo al menos una vez al año en los servicios de SVA de ECERT.

Las evaluaciones técnicas del INDECOPI se llevarán a cabo una vez al año y cada vez que el INDECOPI lo requiera.

14.2 Calificaciones de los auditores

La selección de los auditores depende de lo establecido por el INDECOPI.

14.3 Relación del auditor con el SVA

Los auditores o asesores deben ser independientes de la SVA de ECERT.

15 MATERIAS DE NEGOCIO Y LEGALES

15.1 Tarifas

Las tarifas por los servicios de registro y certificación digital serán definidas directamente con sus clientes B2B.

15.2 Políticas de reembolso

Los servicios de SVA de ECERT no son aplicables a procesos de reembolso.

15.3 Cobertura de seguro

ECERT proporciona a sus clientes servicios de registro amparados por la cobertura del Seguro de Responsabilidad de ECERT.

15.4 Provisiones y Garantías

Las garantías por los servicios de registro y certificación digital serán definidas en los contratos de titulares, en relación a errores u omisiones en la identificación del suscriptor, procesamiento de las solicitudes de certificado o de revocación y protección de datos personales provistos.

15.5 Excepciones y garantías

El SVA de ECERT no se responsabiliza en casos de compromiso de la clave en manos del suscriptor, o cualquier solicitud no realizada según los procedimientos definidos en el presente documento.

15.6 Obligaciones de los suscriptores y titulares

Las obligaciones de los suscriptores y titulares se definen en sus respectivos contratos.

En particular los suscriptores y titulares tienen la responsabilidad de solicitar la revocación de sus certificados en casos de compromiso de su clave privada.

15.7 Obligaciones de los terceros que confían

Las obligaciones del tercero que confía son verificar el estado de confiabilidad de los certificados dentro de los términos establecidos en el marco de la IOFE.

15.8 Indemnización

Los servicios de SVA de ECERT no son aplicables a procesos de indemnización.

15.9 Notificaciones y comunicaciones entre los participantes

Los medios de notificación son:

- Correo electrónico de mesa de servicios: mensajeria@ecert.pe
- Correo electrónico Portal empresa: gestordocumental@e-certchile.cl

15.10 Enmendaduras y cambios

Las enmendaduras y cambios mayores a los documentos normativos serán comunicados al INDECOPI y luego de su aprobación serán publicadas en el sitio web https://www.ecertla.com/peru/.

15.11 Resolución de disputas

El procedimiento de resolución de disputas será por medio del correo electrónico brindado por el Suscriptor a través del contrato y el de ECERT customer@ecertla.com.

ECERT tendrá un plazo de 30 días para contestar al reclamo. En el caso que no sea resuelto, el Suscriptor podrá ingresar su reclamo en el libro de reclamaciones según el D.S. Nro. 011-2011-PCM.

15.12 Conformidad con la ley aplicable

ECERT se compromete a cumplir la ley aplicable a las operaciones de registro: las Guías de Acreditación de Servicio de Valor Añadido del INDECOPI, la Ley de Firmas y Certificados Digitales y su Reglamento.

15.13 Subrogación

ECERT no delega sus responsabilidades respecto de las operaciones de registro sobre terceros no autorizados por la IOFE.

15.14 Fuerza mayor

Las cláusulas de fuerza mayor serán definidas en los contratos de los titulares.

15.15 Derechos de propiedad intelectual

ECERT, tiene derechos de propiedad intelectual sobre todos sus documentos normativos, planes, herramientas de software de firma digital y material comercial, y no podrán ser modificados o atribuidos a otra entidad de manera no autorizada.

16 FINALIZACIÓN DEL SVA DE ECERT

Antes de que el SVA termine sus servicios realizará las siguientes medidas:

- Con 30 días de anticipación se informará a todas las organizaciones clientes B2B y suscriptores la finalización de las operaciones del SVA.
- Se pondrá a disponibilidad de todas las organizaciones clientes B2B la información concerniente a su terminación y las limitaciones de responsabilidad.
- Se concluirán los permisos de autorización de funciones de todos los proveedores.
- Las claves privadas de acceso al SVA, incluyendo copias, serán destruidas de manera segura de modo que no pueda ser recuperada.
- Las provisiones sobre término y terminación, así como las cláusulas de supervivencia serán definidas en los contratos de las organizaciones cliente B2B. Además, las modificaciones realizadas deben ser comunicadas a los suscriptores, titulares y terceros que confían.

17 CONFORMIDAD CON LA LEY APLICABLE

ECERT es afecta y cumple con las obligaciones establecidas por la IOFE, conforme a los requerimientos de la Guía de Acreditación de Entidades Prestadoras de Servicios de Valor Añadido, al Reglamento de la Ley de Certificados Digitales, y a la Ley de Firmas y Certificados Digitales – Ley 27269, para el reconocimiento legal de los servicios de valor añadido emitidos bajo las directrices definidas en el presente documento.

18 BIBLIOGRAFÍA

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

19 CONTROL DE VERSIONES

Control de versiones		
Versión	**Fecha**	**Descripción**
1	07-04-2023	Elaboración de documento inicial.
2	11-01-2024	- Se elimina la palabra "enrolados", reemplazándola por la palabra "persona natural o jurídica". - Se agrega dirección y número de teléfono en Perú. - Se homologa el certificado profesional colegiado como persona jurídica, tal como lo tiene BIT4ID. - Se incluye el punto 16) Finalización de la SVA de ECERT.
3	19-01-2024	Se agrega la responsabilidad de almacenamiento de los documentos firmados al usuario, ECERT no custodia documentos.
4	19-02-2025	- Se actualiza url de página web. - Se actualiza correo de mesa de atención - Se actualiza link de Portal Empresa

Fin del documento