Política y Declaración de Prácticas de Registro

ECERTLA

Norma(s) que Aplican	Referencia Normativa	Área Proceso	Código
INDECOPI - SID	3.2.1 Definición de Responsabilidades	GCOM: Gerencia Comercial	PC-GCOM-0002
INDECOPI - ER	3.2.8 Gestión de la seguridad	PPKI: Gestión procesos de productos PKI (FES - FEA)	

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 Entidad de Registro	Gerente General	Responsable Entidad de Registro	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 Empresa. 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, 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 Empresa 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 objeto la descripción de las operaciones y prácticas que utiliza ECERT para la administración de sus servicios como Entidad de Registro o Verificación – ER, en el marco del cumplimiento de los requerimientos de la "Guía de Acreditación de Entidades de Registros o Verificación (ER)" establecida por el INDECOPI.

3 ALCANCE

El alcance de la acreditación cubre los sistemas de registro y verificación remota que utiliza ECERT de manera previa a la entrega de los servicios de firma digital, a fin de solicitar los certificados digitales del tipo de firma remota proporcionados por la Entidad de Certificación de BIT4ID, conforme al D.S. 029-2021-PCM y a la Resolución 118-2021/CFE INDECOPI.

4 DEFINICIONES Y ABREVIACIONES

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.

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.

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.

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.

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.

RENIEC: Registro Nacional de Identificación y Estado Civil.

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, 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 posterior 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 registro digital que ofrece ECERT son provistos por ECERT CHILE.

5.4 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.

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 del 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 corresponderá a la persona jurídica. La atribución de responsabilidad del suscriptor, para tales efectos, corresponde a la misma persona jurídica.

5.5 Suscriptor

Conforme a la IOFE el Suscriptor es el responsable del uso, control y protección de la clave privada, a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente utilizando su clave privada.

5.6 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.

5.7 Tercero que confía

Tercero que confía son todas aquellas personas naturales o jurídicas que deciden aceptar las transacciones de firma digital 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 de un certificado.

5.8 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 SERVICIOS DE CERTIFICACIÓN DIGITAL

ECERT brinda los servicios de verificación y registro de usuarios que solicitan la emisión, revocación y distribución de los certificados digitales provistos por la Entidad de Certificación de BIT4ID.

Los certificados y las prácticas relacionadas a la gestión de su ciclo de vida son descritos en la Declaración de Prácticas y la Política de Certificación de BIT4ID y en la Declaración de Prácticas y la Política de Registro de ECERT:

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

7 RESPONSABILIDADES

7.1 Responsabilidades de ECERT

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.

7.2 Responsabilidades de los titulares y suscriptores

Los usuarios y solicitantes de los certificados digitales provistos por ECERT son responsables de revisar la presente Declaración de Prácticas de Registro, la Declaración de Prácticas de Certificación y las Políticas de Certificación de BIT4ID, para informarse de las características de la plataforma de servicios, infraestructura y procedimientos empleados en la gestión del ciclo de vida de los certificados digitales, Raíz, Intermedios y de usuario final, así como las obligaciones de cada parte.

7.3 Responsabilidades de los terceros que confían

Las obligaciones de los terceros que confían son:

- Verificar el estado de confiabilidad de los certificados dentro de los términos establecidos en el marco de la IOFE.

8 USO DEL CERTIFICADO

8.1 Tipos de Certificado

ECERT comercializa servicios de firma digital que utilizan certificados de firma regidos por esta Declaración de Prácticas de Registro (PC-GCOM-0002), desde plataformas que son de su propiedad o de terceros que se integran al SID - Portal Empresa.

Con todo, ECERT realiza la validación de identidad para solicitar certificados de firma digital a BIT4ID, el cual se encuentra autorizado por el INDECOPI.

Los tipos de certificado emitidos por Ecert son los siguientes:

Categoría	Tipo de certificado	Descripción	Requisitos
PERSONA NATURAL	PERSONA NATURAL	Aquellos certificados que son emitidos a personas que tienen plena capacidad de ejercicio de sus derechos civiles. Las personas naturales asumirán la responsabilidad de titulares y suscriptores de los certificados digitales que adquieren. Este tipo de certificados emitidos pueden ser utilizados de manera distinta según su vigencia. Según esto se subdividen en certificados para usuarios persona natural y jurídica (con periodos de vigencia de 1 a 3 años) y certificados para usuarios de un solo uso (una sola transacción de firma).	1) Documento nacional de identidad o Cédula de extranjería que es recogido de manera online y contrastado contra el servicio de Consulta en Línea del RENIEC, mediante OCR y biometría facial, de manera automática por los sistemas de validación, a fin de reducir la posibilidad de errores humanos durante el los pasos de validación y evitar también la fuga de datos personales puesto que utiliza un canal centralizado para el recojo de información personal.
			2) Formulario online con datos del solicitante que son extraídos directamente del servicio del RENIEC.
			3) Contrato online firmado con firma electrónica durante el proceso de validación.
PERSONA JURÍDICA	PERSONA JURÍDICA CERTIFICADO DE REPRESENTANTE LEGAL	En el certificado digital del representante legal quedarán registrados todos sus atributos o facultades, los cuales le permitirán utilizar el certificado digital en nombre y representación de la persona jurídica.	1) Documento nacional de identidad o Cédula de extranjería que es recogido de manera online y contrastado contra el servicio de Consulta en Línea del RENIEC, mediante OCR y biometría facial, de manera automática por los sistemas de validación, a fin de reducir la posibilidad de errores humanos durante el los pasos de validación y evitar también la fuga de datos personales puesto que utiliza un canal centralizado para el recojo de información personal.
			2) Formulario online con datos del solicitante que son extraídos directamente del servicio del RENIEC.
			3) Vigencia de poder del Representante legal
			4) Ficha RUC
			5) Contrato online firmado con firma electrónica durante el proceso de validación.
	PERSONA JURÍDICA CERTIFICADO DE ATRIBUTOS / EMPLEADO / PERTENENCIA A EMPRESA/PROFESIONAL	Los certificados digitales de los funcionarios o empleados tienen atributos limitados al desenvolvimiento de sus funciones dentro de la persona jurídica. Reciben el nombre de certificados de atributos, o certificado de empleado, o certificado de pertenencia a empresa. Si se tratase de un profesional colegiado, se especificará como "Colegiado".	1) Documento nacional de identidad o Cédula de extranjería que es recogido de manera online y contrastado contra el servicio de Consulta en Línea del RENIEC, mediante OCR y biometría facial, de manera automática por los sistemas de validación, a fin de reducir la posibilidad de errores humanos durante el los pasos de validación y evitar también la fuga de datos personales puesto que utiliza un canal centralizado para el recojo de información personal.
			2) Formulario con datos del solicitante que son extraídos directamente del servicio del RENIEC
			3) Vigencia de poder del Representante legal
			4) Ficha RUC emitida por SUNAT
			5) Contratos firmados (Representante y empleado)
			6) En el caso de profesionales se debe solicitar la constancia de habilidad profesional que puede ser adjuntada a la solicitud online.
	PERSONA JURÍDICA FIRMA DE AGENTES AUTOMATIZADOS	Los certificados digitales solicitados por personas jurídicas para su utilización a través de agentes automatizados, conocidos también como sistemas transaccionales. La titularidad de certificados y firmas digitales generadas a partir de dicho certificado digital corresponderá a la persona jurídica.	1) Documento nacional de identidad o Cédula de extranjería que es recogido de manera online y contrastado contra el servicio de Consulta en Línea del RENIEC, mediante OCR y biometría facial, de manera automática por los sistemas de validación, a fin de reducir la posibilidad de errores humanos durante el los pasos de validación y evitar también la fuga de datos personales puesto que utiliza un canal centralizado para el recojo de información personal.
			2) Formulario con datos del solicitante que son extraídos directamente del servicio del RENIEC
			3) Vigencia de poder del Representante legal
			4) Ficha RUC emitida por SUNAT
			5) Contrato de certificado de agente automatizado firmado

8.2 Usos adecuados del certificado

Los certificados solicitados por la Entidad de Registro de ECERT tienen las siguientes restricciones de uso:

- Solamente pueden ser utilizados para realizar transacciones de firma dentro de la plataforma Portal Empresa.
- Solamente se emiten certificados, cuyas claves son protegidas en el sistema de firma digital de Bit4ID autorizado por el INDECOPI.
- Los certificados de un solo uso solo pueden ser utilizados para una transacción de firma dentro de Portal Empresa, luego de ello serán revocados.

Otras restricciones respecto del uso adecuado de los certificados son especificadas en las Políticas de Certificación de BIT4ID. Cada política de certificación está identificada por un único identificador de objeto (OID) que además incluye el número de versión.

Los Certificados emitidos bajo dichos documentos pueden ser utilizados con los siguientes propósitos:

- Identificación del Titular: El Titular del Certificado puede autenticar, frente a otra parte, su identidad, demostrando la asociación de su clave privada con la respectiva clave pública, contenida en el Certificado.
- Integridad del documento firmado: La utilización del Certificado garantiza que el documento firmado es íntegro, es decir, garantiza que el documento no fue alterado o modificado después de firmado por el Titular. Se certifica que el mensaje recibido por el Receptor o Destino que confía es el mismo que fue emitido por el Titular.
- No repudio de origen: Con el uso de este Certificado también se garantiza que la persona que firma el documento no puede repudiarlo, es decir, el Titular que ha firmado no puede negar la autoría o la integridad del mismo.

8.3 Usos prohibidos del certificado y exclusión de responsabilidad

Los certificados sólo podrán ser empleados para los usos que hayan sido emitidos y especificados en el presente documento y concretamente en las Políticas de Certificación de BIT4ID.

Se consideran indebidos aquellos usos que no están definidos en el presente documento y en la Declaración de Prácticas de Certificación de BIT4ID.

En consecuencia, para efectos legales, las empresas BIT4ID y ECERT queda eximidas de toda responsabilidad por el empleo de los certificados en operaciones que estén fuera de los límites y condiciones establecidas para el uso de certificados digitales según el presente documento.

9 PERSONA DE CONTACTO

Datos de la Entidad de Registro:

- Nombre: Priscila Evelyn Pérez Vega
- 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
- Teléfono Chile: +56 9 7528 9095
- Correo electrónico: pperez@ecertla.com
- Página Web: https: //www.ecertla.com/peru/

10 ORGANIZACIÓN QUE ADMINISTRA LOS DOCUMENTOS RPS

ECERT administra los documentos de Declaración de Prácticas y todos los documentos normativos de la ER de ECERT.

Para cualquier consulta contactar:

- Nombre: Ignacio Vásquez

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

11 PUBLICACIÓN DE LA DECLARACIÓN DE PRÁCTICAS

La Declaración de Prácticas de Registro - RPS de ECERT, así como la Política de Seguridad, Política y Plan de Privacidad de la Entidad de Registro, y otra documentación relevante son publicadas en la siguiente dirección:

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

Asimismo, la Declaración de Prácticas y Política de Certificación de BIT4ID y otra documentación relevante son publicadas en la siguiente dirección:

- www.uanataca.com/pe

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 de la ER 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 RPS u otra documentación relativa serán publicadas luego de ser aprobadas por el INDECOPI.

11.1 Frecuencia de publicación

ECERT publica de forma inmediata en su página web: 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 auditorias anuales de cumplimiento.

12 IDENTIFICACIÓN Y AUTENTICACIÓN

12.1 Nombres

12.1.1Tipos de nombres

La información relativa a este apartado se encuentra detallada en la Declaración de Prácticas y Política de Certificación de BIT4ID.

12.1.2Necesidad de que los nombres tengan significado

La información relativa a este apartado se encuentra detallada en la Declaración de Prácticas y Política de Certificación de BIT4ID.

12.1.3Modalidades de atención

Para ambos casos, tanto certificados de personas naturales y jurídicas, la solicitud debe ser realizada mediante un contrato de adquisición de los servicios de firma digital de Portal Empresa.

12.2 Solicitud de certificados de persona natural

12.2.1Servicios brindados

La ER de ECERT brinda los siguientes servicios a personas naturales:

a) Atención de solicitudes de bolsas de firmas digitales remotas a través de la plataforma Portal Empresa, que conlleva la emisión de certificados digitales persona natural y jurídica de nacionalidad peruana.
b) Atención de solicitudes de bolsas de firmas digitales remotas a través de la plataforma Portal Empresa, que conlleva la emisión de certificados digitales de un solo uso para personas naturales de nacionalidad peruana.

12.2.2Solicitud de certificados de persona natural

Los clientes de ECERT pueden solicitar sus paquetes de firma en cualquiera de las modalidades de atención especificadas en el presente documento.

Como parte de dicho paquete, la ER solicitará un certificado de firma digital del tipo enrolado a nombre de cada firmante asignado por el cliente (previa validación de identidad), para lo cual la persona natural firmante deberá portar el original de un documento oficial de identidad, el mismo que deberá estar en vigor en la fecha de realización del proceso de registro. No se admitirán fotocopias u otro tipo de documento.

Durante el proceso de validación se tomarán evidencias en formato video y fotografía.

12.2.3Solicitud de certificados de un uso

Los clientes de ECERT pueden solicitar sus paquetes de firma de un solo uso en cualquiera de las modalidades de atención especificadas en el presente documento.

Como parte de dicho paquete, la ER solicitará un certificado de firma digital de un solo uso a nombre de cada firmante asignado por el cliente (previa validación de identidad), para lo cual la persona natural firmante deberá portar el original de un documento oficial de identidad, el mismo que deberá estar en vigor en la fecha de realización del proceso de registro. No se admitirán fotocopias u otro tipo de documento.

Durante el proceso de validación se tomarán evidencias en formato video y fotografía.

12.2.4Autorizados para realizar la solicitud

La solicitud solo puede ser realizada por empresas que tengan contratadas las suscripciones de firma de la plataforma Portal Empresa.

12.2.5Modalidades de atención

Los paquetes de firma pueden ser contratados por personas jurídicas. Los cuales, podrán a su vez, invitar a personas naturales a realizar procesos de firma.

Como parte de los procesos de firma, se solicitarán certificados digitales a nombre, bajo autorización y con previa validación de identidad de la persona natural invitada a firmar.

Sólo se podrán emitir certificados y realizar firmas, si es exitoso el resultado del proceso de validación de identidad, se firma el contrato del suscriptor, se firma la autorización por parte de la Entidad de Registro y se recogen las evidencias correspondientes.

12.2.6Contrato del suscriptor

El suscriptor (persona natural) realizará la aceptación de los Términos y Condiciones, que en adelante llamaremos “contrato del suscriptor”, el cual contiene las obligaciones que deben cumplir los suscriptores de conformidad con la legislación de la materia, para garantizar el efecto legal de las transacciones realizadas, establecidas por las ER de ECERT en coordinación con la EC, así como las consecuencias de no cumplir con el acuerdo.

Este contrato será enviado mediante correo electrónico al solicitante para luego ser archivado por la ER de ECERT.

A través de dicho contrato el suscriptor deberá declarar tener conocimiento de los términos y condiciones aplicables a los certificados.

Esta aceptación de términos y condiciones deberá realizarse antes de la emisión de los certificados.

En el caso del tipo de firma de un uso el contrato del suscriptor será firmado y visualizado desde Portal Empresa.

12.2.7Verificación de suscriptores

Los aspirantes a suscriptores serán validados mediante la presentación virtual de su documento oficial de identidad, la captura en video y fotografía de su rostro. Toda esta información será recogida por el sistema Portal Empresa, el cual contrastará la información con los datos registrados en el RENIEC, mediante el servicio Consulta en Línea.

12.2.8Periodo de vigencia de los certificados

En el caso de los certificados de personas naturales, existen 2 tipos de vigencia:

Certificados persona natural y jurídica: el periodo de vigencia de los certificados solicitados no deberá exceder el periodo de tres (3) años de acuerdo con la legislación vigente.

Certificados de un solo uso: el certificado se encuentra vigente hasta realizar una transacción de firma, luego de lo cual la EC revocará el certificado.

12.2.9Identificación y autenticación de solicitantes de certificados de persona natural

La información proporcionada por los suscriptores de nacionalidad peruana será validada por la ER de ECERT, a través de un mecanismo automático de consulta a las bases de datos del RENIEC.

De manera general, no se incluirá en los certificados información no verificada del suscriptor o el titular según sea el caso. La IOFE permite una excepción en el caso de la dirección de correo electrónico del suscriptor. En este caso se comprobará que la dirección de correo electrónico que se incluye en el certificado es la que efectivamente desea incluir el solicitante. La ER de ECERT no asumirá la responsabilidad de comprobar la existencia de la cuenta de correo electrónico indicada por el solicitante, ni que la dirección sea única, ni su correcto funcionamiento, siendo todo esto responsabilidad del solicitante.

12.3 Solicitud de certificados de persona jurídica

12.3.1Solicitud de certificados persona jurídica de Atributos/empleados/ Pertenencia Empresas

En el caso de certificados de atributos, la persona jurídica se considera como aspirante a titular del certificado y los empleados vienen a ser los aspirantes a suscriptor.

El titular solicitante de las bolsas de firma en Portal Empresa, deberá especificar en su solicitud, la lista de suscriptores y el tipo de atributo al que corresponderá cada certificado,

diferenciando al representante legal de la persona jurídica de los trabajadores que como parte de su cargo requieren de un certificado digital. Esta lista deberá ser debidamente firmada por el Representante Legal o una persona asignada por él.

12.3.2Solicitud de certificados persona jurídica para agentes automatizados

En el caso que el certificado esté destinado para ser usado por un agente automatizado, la solicitud debe ser hecha por el representante designado por la persona jurídica que requiere las transacciones de firma.

En este caso la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderá a la persona jurídica. La atribución de responsabilidad para tales efectos corresponde al representante legal que en nombre de la persona jurídica solicita el certificado digital.

12.3.3Periodo de vigencia de los certificados

En el caso de los certificados de personas naturales, existen 2 tipos de vigencia:

Certificados persona natural y jurídica: el periodo de vigencia de los certificados solicitados no deberá exceder el periodo de tres (3) años de acuerdo con la legislación vigente.

Certificados de un solo uso: el certificado se encuentra vigente hasta realizar una transacción de firma, luego de lo cual la EC revocará el certificado.

12.3.4Reconocimiento, Autenticación y rol de las marcas registradas

Los solicitantes de certificados de personas jurídicas no deben incluir nombres en las solicitudes que puedan suponer infracción de derechos de terceros. La ER de ECERT tiene el derecho de rechazar una solicitud de certificado a causa de conflicto de nombres, puesto que no se podrá volver a asignar un nombre de titular que ya haya sido asignado a un titular diferente.

Mediante la verificación de la documentación e información presentada por el solicitante contra los Registros Públicos o la embajada correspondiente, la ER de ECERT determinará la

validez del nombre de la persona jurídica. Sin embargo, no le corresponde a la ER de ECERT, determinar si un solicitante de certificados le asiste algún tipo de derecho sobre el nombre que aparece en una solicitud de certificado, asimismo, no le corresponde resolver ninguna disputa concerniente a la propiedad de nombres de personas naturales o jurídicas, nombres de dominio, marcas o nombres comerciales.

12.3.5 Identificación y autenticación de solicitantes de certificados de persona jurídica

La persona jurídica deberá acreditar su existencia y su vigencia mediante los instrumentos públicos o norma legal respectiva con el documento de vigencia respectivo expedido por los Registros Públicos o mediante la especificación de la norma legal de creación de la persona jurídica correspondiente. La información proporcionada por los solicitantes será validada por la ER a través de la consulta a la Superintendencia Nacional de los Registros Públicos (SUNARP).

En el caso de empresas constituidas en el extranjero, se acreditará su existencia y vigencia mediante un certificado de vigencia de la sociedad u otro instrumento equivalente expedido por la autoridad competente en su país de origen.

12.3.6 Contrato del titular

El Representante Legal de la persona jurídica o una persona asignada por él, debidamente acreditada, deberá firmar un contrato, que en adelante llamaremos “contrato del titular”.

A través de dicho contrato, el titular deberá declarar tener conocimiento de los términos y condiciones aplicables a los certificados.

La celebración de dicho contrato deberá realizarse antes de la emisión de los certificados de sus suscriptores.

12.3.7Verificación de suscriptores

Los aspirantes a suscriptores deben ser validados de manera remota por medio de una verificación biométrica facial y su DNI contratando contra la base de datos del RENIEC.

El proceso de verificación de sus identidades debe cumplir los requerimientos establecidos en el presente documento respecto de la autenticación de personas naturales.

Cuando un individuo solicite la emisión de un certificado que sirva para acreditar el ejercicio de un cargo en concreto, la ER debe requerir a este solicitante las pruebas que evidencien su cargo, incluyendo la facultad de actuar en nombre de la persona jurídica en la que ocupa dicho cargo. Además, debe presentar el original de su propio documento oficial de identidad.

13 PROCESAMIENTO DE LA SOLICITUD

13.1 Rechazo de la solicitud de emisión de un certificado

La solicitud será rechazada si el solicitante no está capacitado para participar de la comunidad de usuarios de la IOFE:

a) Tratándose de personas naturales, tener plena capacidad de ejercicio de sus derechos civiles.
b) Tratándose de personas jurídicas, acreditar la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva, debiendo contar con un representante debidamente acreditado para tales efectos.

O si el resultado de la validación realizada por la ER fue negativo conforme a lo establecido en este documento.

Una EC puede decidir establecer en su CPS u otra documentación relevante, circunstancias adicionales para el rechazo de la solicitud las cuales serán asumidas por la ER de ECERT.

13.2 Aprobación de la solicitud de emisión de un certificado

En caso de que una solicitud sea aprobada por la ER de ECERT realizará lo siguiente:

Comunicar a la EC su aprobación para la emisión del certificado mediante una comunicación firmada en una conexión segura entre el sistema de registro de Portal Empresa, y los sistemas EC y certificados de firma de Bit4ID.

13.3 Registro de documentos

La ER de ECERT registrará y archivará la solicitud, los contratos firmados y los documentos de sustento presentados por el solicitante. Estos documentos serán protegidos contra acceso no autorizado y destrucción conforme a la Política de Seguridad.

13.4 Método para probar la posesión de la clave privada

La generación del par de claves se realiza bajo control remoto exclusivo y responsabilidad no transferible del suscriptor en el ambiente de certificados de firma de Bit4ID.

El proceso de petición segura del certificado depende de la EC proveedora de los certificados digitales de firma.

13.5 Tiempo para el procesamiento de la solicitud de un certificado

Una vez validada la información proporcionada por el suscriptor, si el resultado de la validación es positivo, la ER de ECERT enviará a la respectiva EC la autorización de la emisión del certificado de manera inmediata.

13.6 Emisión del certificado

La generación de claves y la emisión del certificado será realizada mediante el sistema de firma de Bit4ID.

14 PROCESAMIENTO DE LA SOLICITUD DE REVOCACIÓN

La solicitud de revocación de un certificado digital debe ser realizada por medios no repudiables, a fin de garantizar su autenticidad y no repudio, no es indispensable la solicitud presencial. No puede utilizarse el certificado expirado o revocado para realizar la solicitud.

La Entidad de Registro de ECERTLA S.A.C. comprueba la identidad del solicitante a través de su nombre de usuario y correo electrónico registrado al momento de la generación del certificado.

14.1 Servicios brindados

La Entidad de registro de ECERTLA S.A.C. brinda los siguientes servicios:

- Atención de solicitudes de revocación de certificados para personas naturales
- Atención de solicitudes de revocación de certificados para personas jurídicas

14.2 Autorizados para realizar la solicitud

De acuerdo a lo estipulado por la ley, el tipo de personas que pueden solicitar la revocación de un certificado son:

- Titular del certificado
- Suscriptor del certificado
- La EC o ER que emitió el certificado
- Un juez que de acuerdo a la ley decida revocar el certificado.
- Un tercero que tenga pruebas fehacientes del uso indebido del certificado.

14.3 Identificación y autenticación de los solicitantes

Los suscriptores deberán presentar ante la ER su documento oficial de identidad.

Los titulares deberán presentar documentos que acrediten dicha representación y la voluntad de dicha persona jurídica.

Los terceros (diferentes de la EC, el suscriptor y el titular) deberán presentar ante la ER pruebas fehacientes del uso indebido del certificado de acuerdo a la ley vigente, junto a la orden judicial respectiva.

14.4 Modalidades de atención

El cliente tiene dos alternativas para poder gestionar su solicitud de revocación de certificado:

a) De manera directa: Un usuario persona natural y/o jurídica que necesita revocar su certificado debe seguir los siguientes pasos:

Paso 1: ingresar al siguiente link https://www.ecertla.com/peru/

Paso 2: Pulsa Revocar certificado. Al pulsar este enlace se redirige a https://www.uanataca.com/lcmpl/

Paso 3: Los requisitos para generar la solicitud son ingresar Usuario y ERC.

Paso 4: El certificado se revoca de manera automática.

b) A través de la Entidad de Registro: En el caso de que el usuario persona natural y/o jurídica necesite asistencia del personal de ecert debe seguir los siguientes pasos:

Paso 1: El Cliente o un tercero solicita la revocación de certificado a través del siguiente correo electrónico: pperez@ecertla.com, indicando el motivo de revocación, para ello deberá adjuntar:

- Documento de identidad
- Correo electrónico asociado al certificado digital
- RUC de la empresa asociada de ser el caso

Para el caso de Certificado pertenencia empresa, el solicitante de la revocación deberá adjuntar un poder simple firmado digitalmente por el representante legal de la empresa. Además, deberá adjuntar el listado de usuarios indicando DNI, Correo electrónico asociado al certificado y motivo de revocación.

Paso 2: La Entidad de registro una vez verificada la identidad del solicitante procederá a enviar el usuario y código ERC al solicitante con las instrucciones que debe seguir.

14.4.1Solicitud de revocación de certificados de persona natural

El solicitante deberá especificar en su solicitud el motivo de revocación adjuntando su documento oficial de identidad.

Una vez que el certificado haya sido revocado, le llegará un correo de confirmación.

14.4.2Solicitud de revocación de certificados de persona jurídica

El solicitante deberá especificar en su solicitud indicando explícitamente lo siguiente:

Datos de la empresa: RUC, Razón social

Datos del suscriptor: DNI, Tipo de firma, motivo de revocación, los cuales pueden ser:

- No especificado.
- Clave comprometida.
- Cambio de vínculo.
- Por sustitución.
- Cese de actividad.
- Poderes retirados.

Esta lista deberá ser debidamente firmada por el Representante Legal o una persona asignada por él.

Una vez que el certificado haya sido revocado, le llegará un correo de confirmación.

14.4.3Solicitud de revocación de certificados para agentes automatizados

En el caso que el certificado esté destinado para ser usado por un agente automatizado, la solicitud debe ser hecha por el representante legal designado por la persona jurídica dueña del certificado.

Una vez que el certificado haya sido revocado, le llegará un correo de confirmación.

14.5 Rechazo de la revocación

La solicitud de revocación de certificado será rechazada en caso no se cumpla con alguna de las modalidades de solicitud o que el

solicitante no se encuentre debidamente autorizado conforme a lo descrito en el presente documento.

Adicionalmente, la solicitud será rechazada si el solicitante no está capacitado para participar de la comunidad de usuarios de la IOFE:

1) Tratándose de personas naturales, tener plena capacidad de ejercicio de sus derechos civiles.
2) Tratándose de personas jurídicas, acreditar la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o

norma legal respectiva, debiendo contar con un representante debidamente acreditado para tales efectos.

O si el resultado de la validación realizada por la ER fue negativo, conforme a lo establecido en este documento.

14.6 Registro de documentos

La ER de ECERT registrará y archivará el correo de solicitud de revocación y los documentos de sustento presentados por el solicitante dejando constancia de la persona que efectúa la solicitud, la relación que tiene ésta con el titular, las razones de la solicitud, las acciones tomadas para la verificación de la veracidad de la solicitud.

Estos documentos serán protegidos contra acceso no autorizado y destrucción conforme a la Política de Seguridad.

En caso de que no se acepte la revocación, se dejará constancia de los hechos que motivaron dicha denegatoria.

En el caso de solicitudes realizadas directamente al servicio online de la EC, ECERT no almacenará ninguna evidencia.

14.7 Tiempo para el procesamiento de la solicitud de revocación

Una vez validada la información proporcionada por el suscriptor, si el resultado de la validación es positivo, la ER de ECERT enviará un correo electrónico indicando al solicitante los paso a seguir descritos en el punto 15.4 de la presente declaración.

El máximo tiempo de respuesta para la revocación del certificado dependerá de lo establecido en la CP y CPS de la EC.

En el caso de solicitudes realizadas directamente al servicio online de la EC, ECERT no participará del procesamiento de solicitud de revocación.

14.8 Revocación del certificado

La revocación del certificado se realizará conforme a la política de certificación de la EC de Bit4ID.

15 RE-EMISIÓN DEL CERTIFICADO

ECERT no realiza el proceso de re-emisión del certificado.

16 SUSPENSIÓN DEL CERTIFICADO

ECERT no realiza el proceso de suspensión del certificado.

17 DE GOBIERNO

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

- El Gerente General debe:
- Asegurar el establecimiento de esta Práctica, así como de su adecuación a los procesos de negocio.

- Revisar al menos una vez al año esta Práctica, revisión que debe ser aprobada por el mismo Gerente General.
- Informar al Directorio y los ejecutivos de la empresa, por sí mismo o por quién éste designe.
- El Comité Sistema de Gestión debe:
- Asegurar la implementación de esta Práctica, para lo cual le corresponde hacer seguimiento de la gestión de riesgos y oportunidades en cada sesión.
- Informar al Gerente General y a la plana ejecutiva de los riesgos asociados a esta Práctica y su implementación, así como resolver respecto de las medidas de mitigación.
- El Propietario del Proceso, del Riesgo o del Activo de Información, debe:
- Asegurar la aplicación y seguimiento de Práctica y los documentos relacionados.
- Planificar sus procesos, objetivos e indicadores, de forma coherente con la presente Práctica, con la finalidad de minimizar los riesgos, gestionar las oportunidades, verificar el desempeño y optimizar los resultados de la organización en su conjunto.

18 FINALIZACIÓN DE LA ER DE ECERT

Antes de su finalización, la ER de ECERTLA informará a los suscriptores, titulares y terceros que confían sobre el cese de sus operaciones con por lo menos 30 días calendario de anticipación. Y 60 días de anticipación en caso de la Autoridad Administrativa Competente.

Todos los expedientes de solicitud de certificados existentes serán transferidos al INDECOPI o a otro PSC designado por este en cumplimiento de las garantías y responsabilidades previamente establecidas.

Asimismo, ECERTLA indicará que, de no existir objeción a la transferencia de los certificados a otro certificador, dentro del plazo de 15 días hábiles contados desde la fecha de la comunicación, se entenderá que el usuario ha consentido en la transferencia de estos.

En caso de una operación de trasferencia de titularidad, los nuevos dueños u operadores solicitaran la evaluación de cumplimiento al INDECOPI para garantizar que se mantienen los

requisitos de acreditación. Se advertirá a todos los suscriptores, titulares y personas que confían respecto a los cambios y todo tipo de condición asociada a la continuidad del uso de los certificados emitidos por una Entidad Certificadora que finaliza o transfiere sus operaciones, mediante un comunicado publicado en la siguiente dirección:

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

19 TARIFAS

Las tarifas por los servicios de registro serán definidas directamente con el cliente.

20 NOTIFICACIONES Y COMUNICACIONES ENTRE PARTICIPANTES

Los medios de notificación son:

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

21 CONTEXTO NORMATIVO

La presente Práctica de ECERT debe cumplir las exigencias de la normativa y estandarización vigente:

1) Guía de Acreditación de Entidades de Registro o Verificación, INDECOPI
2) Ley de Firmas y Certificados Digitales – Ley 27269
3) Decreto Supremo 052-2008
4) Decreto Supremo 070-2011

22 FRECUENCIA DE PUBLICACIÓN

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

https://www.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.

23 PUBLICACIÓN

ECERT publica de forma inmediata en su página web: 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.

24 SENSIBILIZACIÓN 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.

25 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 a los clientes de los clientes y/o que manifiesten como quejas del cliente o de INDECOPI, deben ser informados al Gerente General y al Directorio de ECERT.

26 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 Práctica, dependiendo del tipo de incumplimiento se debe amonestar o rescindir el contrato.

27 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" se reemplaza por Persona natural, persona 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 19) Finalización de la ER de ECERT.
3	18-01-2024	- Se elimina la palabra "firma remota " se reemplaza por certificados de firma.
4	19-02-2025	- Se actualiza la url de página web - Se actualizan cargo y correo electrónico de responsable de Seguridad y Privacidad - Se actualiza correo de mesa de servicios. - Se actualiza sección 13.2.6 donde se especifica que el contrato del suscriptor será enviado por Correo electrónico y en el caso del tipo de firma de un uso el contrato del suscriptor será firmado y visualizado desde Portal Empresa.

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.