IDENTITY DEL PERU SOCIEDAD ANONIMA

ENTIDAD DE REGISTRO O VERIFICACION

DECLARACION DE PRÁCTICAS Y POLÍTICAS DE REGISTRO DE IDENTITY DEL PERU S.A. VERSIÓN 1.1

D1.1.2024

Elaborado y aprobado por:	Gerencia de Registro Digital de la ER Identity del Peru SA
Dirigido a:	Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI)
Tipo de Documento:	Declaración de Prácticas y Políticas de Registro
Versión:	1.1
Fecha de elaboración:	25/04/2024

CONTROL DE VERSIONES

Versión	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
1.0	Original	Creación del documento	ACC / BSC	01/03/2024
1.1	12 12.1.7 12.1.8 12.1.9 12.1.10 12.2.3 12.2.5 12.2.6 13.4 14 14.1.1 14.2.1 15.4 18.1.6	Ajuste de los perfiles de certificados Se ha agregado el protocolo de comunicación entre la ER y la EC	BSC	25/04/2024

ÍNDICE

1. INTRODUCCIÓN..... Pág. 6
2. OBJETIVO..... Pág. 6
3. DEFINICIONES Y ABREVIACIONES..... Pág. 6-7
4. DIFERENCIACIÓN DE LOS PARTICIPANTES..... Pág. 7
   4.1 ENTIDAD DE CERTIFICACIÓN – EC..... Pág. 7
   4.2 ENTIDAD DE REGISTRO – ER ..... Pág. 7
   4.3 PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN DIGITAL ..... Pág. 8
   4.4 TITULAR DE CERTIFICADO DIGITAL..... Pág. 8
   4.5 SUSCRIPTOR DE CERTIFICADO DIGITAL..... Pág. 8
   4.6 SOLICITANTE DE CERTIFICADO DIGITAL..... Pág.8
   4.7 TERCERO QUE CONFÍA O TERCER USUARIO..... Pág. 8
   4.8 ENTIDAD A LA CUAL SE ENCUENTRA VINCULADO EL TITULAR DE CERTIFICADO DIGITAL..... Pág. 8
5. RESPONSABILIDAD LEGAL..... Pág. 9
6. USO DEL CERTIFICADO DIGITAL
   6.1 USOS ADECUADOS DEL CERTIFICADO DIGITAL..... Pág. 9
   6.2 USOS PROHIBIDOS / NO AUTORIZADOS, Y EXONERACIÓN DE RESPONSABILIDAD..... Pág. 9
7. INFORMACIÓN DE CONTACTOS..... Pág. 9-10
8. ORGANIZACIÓN QUE ADMINISTRA LOS DOCUMENTOS DE RPS..... Pág. 10
9. RESPONSABILIDADES DE LOS TITULARES Y/O SUSCRIPTORES..... Pág. 10
10. PUBLICACIÓN DE LA DECLARACIÓN DE PRÁCTICAS Y OTROS DOCUMENTOS..... Pág. 10
11. IDENTIFICACIÓN Y AUTENTICACIÓN
   11.1NOMBRES..... Pág. 11
      11.1.1 TIPOS DE NOMBRES..... Pág. 11
      11.1.2 PSEUDÓNIMOS..... Pág. 11
      11.1.3 REGLAS UTILIZADAS PARA INTERPRETAR VARIOS FORMATOS DE NOMBRES..... Pág. 11
      11.1.4 UNICIDAD DE LOS NOMBRES..... Pág. 11
      11.1.5 RECONOCIMIENTO, AUTENTICACIÓN Y FUNCIÓN DE LAS MARCAS REGISTRADAS..... Pág. 11
      11.1.6 MÉTODOS DE PRUEBA DE LA POSESIÓN DE LA CLAVE PRIVADA..... Pág. 11
      11.1.7 AUTENTICACIÓN DE LA IDENTIDAD DE UN INDIVIDUO LA ENTIDAD Y SU VINCULACIÓN..... Pág. 11
12. SOLICITUD DE EMISIÓN DE CERTIFICADOS DIGITALES
   12.1SOLICITUD DE CERTIFICADOS DE PERSONA JURÍDICA..... Pág. 11
      12.1.1 SERVICIOS BRINDADOS POR IDENTITY..... Pág. 11-12
      12.1.2 PERSONAS AUTORIZADAS PARA REALIZAR LA SOLICITUD..... Pág. 12
      12.1.3 FORMAS DE ATENCIÓN..... Pág. 12
      12.1.4 SOLICITUD DE CERTIFICADOS

DE ATRIBUTOS..... Pág. 12-13
12.1.5 SOLICITUD DE CERTIFICADOS PARA AGENTES AUTOMATIZADOS..... Pág. 13
12.1.6 VIGENCIA DE LOS CERTIFICADOS..... Pág. 13
12.1.7 RECONOCIMIENTO, AUTENTICACIÓN Y FUNCIÓN DE LAS MARCAS REGISTRADAS..... Pág. 13
12.1.8 IDENTIFICACIÓN Y AUTENTICACIÓN DE SOLICITANTES DE CERTIFICADOS DE PERSONA JURÍDICA..... Pág. 13-14
12.1.9 CONTRATO DE SUSCRIPTOR..... Pág. 14
12.1.10 VERIFICACIÓN DEL SUSCRIPTOR..... Pág. 14
12.2SOLICITUD DE CERTIFICADOS DE PERSONA NATURAL..... Pág. 14
12.2.1 SERVICIOS BRINDADOS POR IDENTITY..... Pág. 14
12.2.2 PERSONA AUTORIZADA PARA REALIZAR LA SOLICITUD..... Pág. 15
12.2.3 FORMAS DE ATENCIÓN..... Pág. 15
12.2.4 SOLICITUD DE CERTIFICADOS DE PERSONA NATURAL..... Pág. 15
12.2.5 CONTRATO DE SUSCRIPTOR..... Pág. 15
12.2.6 VERIFICACIÓN DEL SUSCRIPTOR..... Pág. 15
12.2.7 VIGENCIA DE LOS CERTIFICADOS..... Pág. 16
12.2.8 IDENTIFICACIÓN Y AUTENTICACIÓN DE SOLICITANTES DE CERTIFICADOS DE PERSONA NATURAL..... Pág. 16
13. PROCESAMIENTO DE LA SOLICITUD
13.1 RECHAZO DE LA SOLICITUD DE EMISIÓN DE UN CERTIFICADO..... Pág. 16
13.2 APROBACIÓN DE LA SOLICITUD DE EMISIÓN DE UN CERTIFICADO..... Pág. 16
13.3 REGISTRO DE DOCUMENTOS..... Pág. 17
13.4 MÉTODO PARA PROBAR LA POSESIÓN DE LA CLAVE PRIVADA..... Pág. 17
13.5 TIEMPO PARA EL PROCESAMIENTO DE LA SOLICITUD DE UN CERTIFICADO..... Pág. 17
13.6 EMISIÓN DEL CERTIFICADO..... Pág. 17
14. SOLICITUD DE RE-EMISIÓN DE CERTIFICADOS DIGITALES..... Pág. 17
14.1 SOLICITUD DE RE-EMISIÓN DE CERTIFICADOS PARA PERSONA JURIDICA..... Pág. 17
14.1.1 SERVICIOS BRINDADOS POR IDENTITY..... Pág. 17-18
14.1.2 PERSONAS AUTORIZADAS PARA REALIZAR LA SOLICITUD..... Pág. 18
14.1.3 FORMAS DE ATENCIÓN..... Pág. 18
14.1.4 SOLICITUD DE RE-EMISIÓN DE CERTIFICADOS DE ATRIBUTOS..... Pág. 18
14.1.5 IDENTIFICACIÓN Y AUTENTICACIÓN DE SOLICITANTES DE RE-EMISIÓN DE CERTIFICADOS DE PERSONA JURÍDICA..... Pág. 19
14.2 SOLICITUD DE RE-EMISIÓN DE CERTIFICADOS DE PERSONA NATURAL..... Pág. 19
14.2.1 SERVICIOS BRINDADOS POR IDENTITY..... Pág. 19
14.2.2 PERSONA AUTORIZADA PARA REALIZAR LA SOLICITUD..... Pág. 19
14.2.3 FORMAS DE ATENCIÓN..... Pág. 19-20

14.2.4 SOLICITUD DE CERTIFICADOS DE PERSONA NATURAL..... Pág. 20
14.2.5 IDENTIFICACIÓN Y AUTENTICACIÓN DE SOLICITANTES DE CERTIFICADOS DE PERSONA NATURAL..... Pág. 20
15. PROCESAMIENTO DE LA SOLICITUD DE RE-EMISIÓN..... Pág. 20
15.1 RECHAZO DE LA SOLICITUD DE EMISIÓN DE UN CERTIFICADO..... Pág. 20
15.2 APROBACIÓN DE LA SOLICITUD DE EMISIÓN DE UN CERTIFICADO..... Pág. 20
15.3 REGISTRO DE DOCUMENTOS..... Pág. 21
15.4 MÉTODO PARA PROBAR LA POSESIÓN DE LA CLAVE PRIVADA..... Pág. 21
15.5 TIEMPO PARA EL PROCESAMIENTO DE LA SOLICITUD DE UN CERTIFICADO..... Pág. 21
15.6 RE-EMISIÓN DEL CERTIFICADO..... Pág. 21
16. SOLICITUD DE REVOCACIÓN DE CERTIFICADOS..... Pág. 21
16.1 SITUACIONES PARA REALIZAR LA SOLICITUD..... Pág. 21
16.2 SOLICITUD DE REVOCACIÓN DE CERTIFICADOS..... Pág. 22
16.2.1 SERVICIOS BRINDADOS POR IDENTITY..... Pág. 22
16.2.2 PERSONAS AUTORIZADAS PARA REALIZAR LA SOLICITUD..... Pág. 22
16.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS SOLICITANTES..... Pág. 22-23
16.2.4 FORMAS DE ATENCIÓN..... Pág. 23
16.2.5 SOLICITUD DE REVOCACIÓN DE CERTIFICADOS DE ATRIBUTOS..... Pág. 23
16.2.6 SOLICITUD DE REVOCACIÓN DE CERTIFICADOS PARA AGENTES AUTOMATIZADOS..... Pág. 23
16.2.7 SOLICITUD DE REVOCACIÓN DE CERTIFICADOS DE PERSONA NATURAL..... Pág. 23
17. PROCESAMIENTO DE LA SOLICITUD DE REVOCACIÓN..... Pág. 23
17.1 RECHAZO DE LA SOLICITUD DE REVOCACIÓN..... Pág. 23-24
17.2 APROBACIÓN DE LA SOLICITUD DE REVOCACIÓN..... Pág. 24
17.3 REGISTRO DE DOCUMENTOS..... Pág. 24
17.4 TIEMPO PARA EL PROCESAMIENTO DE LA SOLICITUD DE REVOCACIÓN..... Pág. 24
17.5 REVOCACIÓN DEL CERTIFICADO..... Pág. 24
18. CONTROLES DE LAS INSTALACIONES, DE LA GESTIÓN Y CONTROLES OPERACIONALES..... Pág. 25
18.1CONTROLES FÍSICOS..... Pág. 25
18.1.1 UBICACIÓN Y CONSTRUCCIÓN DEL LOCAL..... Pág. 25
18.1.2 ACCESO FÍSICO..... Pág. 25
18.1.3 ENERGÍA Y AIRE ACONDICIONADO..... Pág. 25
18.1.4 EXPOSICIÓN AL AGUA..... Pág. 25
18.1.5 PREVENCIÓN Y PROTECCIÓN CONTRA FUEGO..... Pág. 25-26
18.1.6 ARCHIVO DE MATERIAL..... Pág. 26
18.1.7 GESTIÓN DE RESIDUOS..... Pág. 26
18.1.8 COPIA DE SEGURIDAD EXTERNA..... Pág. 26
18.2CONTROLES PROCESALES..... Pág. 26
18.2.1 ROLES DE CONFIANZA..... Pág. 26-28

18.2.2 NÚMERO DE PERSONAS REQUERIDAS POR LABOR..... Pág. 28
18.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN POR CADA ROL..... Pág. 28
18.3 CONTROLES DE PERSONAL..... Pág. 28
18.3.1 CUALIDADES Y REQUISITOS, EXPERIENCIA Y CERTIFICADOS..... Pág. 28-29
18.3.2 PROCEDIMIENTOS PARA VERIFICACIÓN DE ANTECEDENTES..... Pág. 29
18.3.3 REQUISITOS DE CAPACITACIÓN..... Pág. 29
18.3.4 FRECUENCIA Y REQUISITOS DE LAS RE-CAPACITACIONES..... Pág. 29-30
18.3.5 FRECUENCIA Y SECUENCIA DE LA ROTACIÓN EN EL TRABAJO..... Pág. 30
18.3.6 SANCIONES POR ACCIONES NO AUTORIZADAS..... Pág. 30
18.3.7 DOCUMENTACIÓN SUMINISTRADA AL PERSONAL DE IDENTITY..... Pág. 30
18.4 GESTIÓN DE OPERACIONES..... Pág. 30
18.4.1 MÓDULO CRIPTOGRÁFICO..... Pág. 30
18.4.2 RESTRICCIONES DE LA GENERACIÓN DE CLAVES..... Pág. 31
18.4.3 ENTREGA DE LA CLAVE PÚBLICA..... Pág. 31
18.4.4 DEPÓSITO DE LA CLAVE PÚBLICA..... Pág. 31
18.4.5 DATOS DE ACTIVACIÓN..... Pág. 31
19. AUDITORÍAS..... Pág. 31
19.1 FRECUENCIA DE AUDITORÍAS..... Pág. 31
19.2 CALIFICACIONES DE LOS AUDITORES..... Pág.31
19.3 RELACIÓN DEL AUDITOR CON LA ER IDENTITY..... Pág. 31
20. MATERIAS DE NEGOCIO Y LEGALES..... Pág. 31
20.1 TARIFAS..... Pág. 31
20.2 POLÍTICAS DE REEMBOLSO..... Pág. 31
20.3 COBERTURA DE SEGURO..... Pág. 32
20.4 PROVISIONES Y GARANTÍAS..... Pág. 32
20.5 EXCEPCIONES DE GARANTÍAS..... Pág. 32
20.6 OBLIGACIONES DE LOS SUSCRIPTORES Y TITULARES..... Pág. 32
20.7 OBLIGACIONES DE LOS TERCEROS QUE CONFÍAN..... Pág. 32
20.8 INDEMNIZACIÓN..... Pág. 32
20.9 NOTIFICACIONES..... Pág. 32
20.10 ENMENDADURAS Y CAMBIOS..... Pág. 32
20.11 RESOLUCIÓN DE DISPUTAS..... Pág. 32
20.12 CONFORMIDAD CON LA LEY APLICABLE..... Pág.32
20.13 SUBROGACIÓN..... Pág.33
20.14 FUERZA MAYOR..... Pág. 33
20.15 DERECHOS DE PROPIEDAD INTELECTUAL..... Pág. 33
21. FINALIZACIÓN DE LA ER IDENTITY..... Pág. 33
22. BIBLIOGRAFÍA..... Pág. 33

1. INTRODUCCIÓN

Identity del Perú Sociedad anónima es una empresa privada reconocida en el mercado nacional que brinda el servicio de Identidad Digital, Comunicaciones Seguras, Venta Licencias de Certificados Digitales destinado a organizaciones, software, servidores y personas naturales, así como representantes legales de empresas, de ser el caso, con el soporte de una Autoridad Certificadora reconocida mundialmente como BIT4ID.

En virtud de un Convenio de Prestación de Servicios, se regulan las condiciones y modalidades de la prestación de servicios por parte de:

- **BIT4ID SA.** (Prestadora de Servicios de Certificación Digital, debidamente acreditada por el INDECOPI), que es una sociedad peruana y,
- **IDENTITY DEL PERU S.A**, que presta los servicios de registro o verificación, tanto de personas naturales como jurídicas, en la demarcación de Lima y otras ciudades del Perú, conforme a lo establecido en la Declaración de Prácticas de Certificación, las Políticas de Certificación de BIT4ID., sus procedimientos y documentos técnicos, así como la Ley N° 27269, y su Reglamento.

Entre los tipos de certificados digitales que Identity provee se encuentran: Certificados digitales de persona jurídica clase III.

2. OBJETIVO

Este documento tiene como objeto la descripción de las operaciones y prácticas que utiliza Identity para la administración de sus servicios como Entidad de Registro o Verificación, en el marco del cumplimiento de los requerimientos de la "Guía de Acreditación de Entidades de Registros o Verificación" establecida por el INDECOPI.

3. DEFINICIONES Y ABREVIACIONES

Entidad de Certificación (EC):	Persona jurídica o privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital. Asimismo, puede asumir las funciones de registro o verificación.
Entidad de Registro o Verificación (ER):	Persona jurídica, con excepción de los notarios públicos, encargada del levantamiento de datos, comprobación de estos respecto a un solicitante de un mecanismo de firma electrónica o certificación digital, la aceptación y autorización de las solicitudes para la emisión de un mecanismo de firma electrónica o certificados digitales, así como de la aceptación y autorización de las solicitudes de cancelación de mecanismos de firma electrónica o certificados digitales. Las personas encargadas de ejercer la citada función serán supervisadas y reguladas por la normatividad vigente.
Declaración de Prácticas de Certificación (CPS):	Documento oficialmente presentado por una entidad de certificación a la Autoridad Administrativa Competente, mediante el cual se define sus Prácticas de Certificación.
Declaración de Prácticas de Registro o Verificación (RPS):	Documento oficialmente presentado por una Entidad de Registro o Verificación a la Autoridad Administrativa Competente, mediante el cual define sus Prácticas de Registro o Verificación.
Identificador de Objeto (OID):	Es una cadena de números, formalmente definida usando el estándar ASN.1 (ITU-T Rec. X.660 ISO/IEC 9834 series), que identifica de forma única a un objeto. En el caso de la

	certificación digital, los OIDs se utilizan para identificar a los distintos objetos en los que ésta se enmarca (por ejemplo, componentes de los Nombres Diferenciados, CPS, etc.).
Infraestructura Oficial de Firma Electrónica (IOFE)	Sistema confiable, acreditado, regulado y supervisado por el INDECOPI, provisto de instrumentos legales y técnicos que permiten generar firmas electrónicas y proporcionar diversos niveles de seguridad respecto a: 1) la integridad de los mensajes de datos y documentos electrónicos; 2) la identidad de su autor, lo que es regulado conforme a la Ley. El sistema incluye la generación de firmas electrónicas, en las que participan entidades de certificación y entidades de registro o verificación acreditadas ante el INDECOPI incluyendo a la Entidad de Certificación Nacional para el Estado Peruano (ECERNEP), las Entidades de Certificación para el Estado Peruano (ECEP) y las Entidades de Registro o Verificación para el Estado Peruano (EREP).
Operador de Registro:	Persona responsable de representar a Identity en calidad de ER de BIT4ID en las actividades de recepción, validación y procesamiento de solicitudes.
Prácticas de Registro o Verificación:	Son las prácticas que establecen las actividades y requerimientos de seguridad y privacidad correspondientes al Sistema de Registro o Verificación de una ER.
Registro Nacional de Identificación y Estado Civil (RENIEC):	Es un organismo autónomo del Estado Peruano, encargado de la identificación de los peruanos, otorgando el Documento Nacional de Identidad (DNI), registrando hechos vitales como nacimientos, matrimonios, defunciones, divorcios y otros que modifican el estado civil. Durante los procesos electorales, proporciona el Padrón Electoral que se utilizará en las elecciones.
Superintendencia Nacional de los Registros Públicos (SUNARP):	Es un organismo autónomo del Estado Peruano, tiene como función la planificación y organización de las inscripciones y publicidades de actos y contratos en los registros de los derechos y titularidades.

4. DIFERENCIACIÓN DE LOS PARTICIPANTES

4.1 ENTIDAD DE CERTIFICACIÓN - EC

La EC BIT4ID, en su calidad de Entidad de Certificación acreditada, presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios vinculados a la certificación digital. Los servicios ofrecidos por la EC BIT4ID comprenden aquellos orientados a la gestión del ciclo de vida de los certificados digitales, de acuerdo con lo especificado en su correspondiente Declaración de Prácticas de Certificación (RPS).

4.2 ENTIDAD DE REGISTRO – ER

Identity, en su calidad de Entidad de Registro, se encarga de validar la información suministrada por un solicitante de certificado digital; mediante la comprobación de sus datos, identificación y autenticación, para su posterior registro. Dentro de estas funciones se debe tener presente la gestión interna ante la EC BIT4ID a fin de que aquella genere o cancele el certificado digital emitido a nombre de un solicitante de certificado digital.

4.3 PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN DIGITAL (AC BIT4ID S.A.[1])

[1] Prestador de Servicios de Confianza (TSP)

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

Los servicios de certificación digital que ofrece Identity son provistos en un contrato de tercerización por la Entidad de Certificación de BIT4ID.

4.4 TITULAR DE CERTIFICADO DIGITAL

Un titular de certificado digital, es aquella persona natural o jurídica a quien se le atribuye de manera exclusiva un certificado digital.

4.5 SUSCRIPTOR DE CERTIFICADO DIGITAL

Un suscriptor de certificado digital, es aquella persona natural responsable de la generación y 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 sea una persona natural, sobre la misma recaerá la responsabilidad de suscriptor.

En el caso que una persona jurídica sea el titular de un certificado, la responsabilidad de suscriptor recaerá sobre el representante legal designado por esta entidad. Si el certificado esta 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 cual deberá ser dueña del agente automatizado. La atribución de responsabilidad de suscriptor, para tales efectos, corresponde al representante legal, que en nombre de la persona jurídica solicita el certificado digital.

4.6 SOLICITANTE DE CERTIFICADO DIGITAL

Se entenderá por Solicitante de un certificado digital, a aquella persona natural o jurídica que solicita un certificado digital, aceptando previamente lo establecido en la CPS de BIT4ID, así como en la RPS de Identity.

En el caso de los certificados de persona natural puede coincidir con la figura del Titular de un certificado digital.

4.7 TERCERO QUE CONFÍA O TERCER USUARIO

Se considerará como Tercero que Confía o Tercer Usuario, a aquellas personas naturales, equipos, servicios o cualquier otro ente que actúa basado en la confianza sobre la validez de un certificado y/o verifica alguna firma digital en la que se utilizó dicho certificado.

4.8 ENTIDAD A LA CUAL SE ENCUENTRA VINCULADO EL TITULAR DE CERTIFICADO DIGITAL

Se considerará como Entidad a la cual se encuentra vinculado el Titular de un Certificado Digital, a la persona jurídica u organización que mantiene un vínculo con el Titular de un certificado digital.

5 RESPONSABILIDAD LEGAL

Las responsabilidades contractuales, garantías financieras y coberturas de seguros son brindadas por AC BIT4ID de acuerdo con su CPS.

Identity, brinda los servicios de registro o verificación conforme a las Guías de Acreditación del INDECOPI, para realizar la verificación de identidad de las personas jurídicas y naturales solicitantes de los certificados digitales. Las solicitudes, quejas o reclamos (sean virtuales o físicas) sobre los servicios prestados son recibidos directamente por Identity.

La atención telefónica brindada por Identity a todos los participantes descritos en el punto 4, es permanente.

6 USO DEL CERTIFICADO DIGITAL

6.1 USOS ADECUADOS DEL CERTIFICADO DIGITAL

El uso de los certificados digitales está determinado en la CPS de la EC BIT4ID.

En términos generales, se admiten los certificados para los siguientes usos:

- **Identificación del Titular**: El Titular del certificado puede autenticar, frente a otro individuo, su identidad, demostrando la asociación de su clave privada con la respectiva clave pública.
- **Identidad del documento firmado**: La utilización del certificado otorga plena seguridad de que el documento firmado es integro. Vale decir, que no fue alterado o modificado, después de que el Titular lo firmó.
- **No repudio:** Con el uso de este certificado, se garantiza además, que el individuo que firma el documento no podrá repudiarlo. Vale decir, que el Titular que firmó este documento no podrá negar su autoría, o la integridad del mismo.

Cada política de certificación está identificada por un único identificador de objeto (OID) que además incluye el número de versión.

6.2 USOS PROHIBIDOS / NO AUTORIZADOS, Y EXONERACIÓN DE RESPONSABILIDAD

Los certificados sólo podrán ser empleados para los usos para los que hayan sido emitidos en cada caso, y que vienen descritos en las políticas de certificación correspondientes (CPS de BIT4ID).

Se consideran indebidos aquellos usos que no están definidos en la CPS de BIT4ID y en consecuencia para efectos legales, tanto BIT4ID como Identity, quedan exonerados 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.

7 INFORMACIÓN DE CONTACTOS

Datos de la Entidad de Certificación y Prestadora de Servicios:

Nombre:	BIT4ID.
Dirección:	CAL.ENRIQUE PALACIOS NRO. 360 URB. SURQUILLO (PISO 5-OFICINA 510) LIMA - LIMA - MIRAFLORES.
Teléfono:	+51 1 242 9994
Correo electrónico:	cmr@bit4id.com
Página Web:	https://www.bit4id.com/es/

Datos de la Entidad de Registro o Verificación:

Nombre:	IDENTITY DEL PERU SOCIEDAD ANONIMA.

Dirección: Calle Las orquídeas 585, Distrito de San Isidro, Provincia y Departamento de Lima.
Teléfono: 01-7390900 / 0800-7-1500
Correo electrónico: brenda.salas@solutitech.com
- Página Web: https://certificacion.soluti.pe/pki/certificateRequest/primerid-cpp

8 ORGANIZACIÓN QUE ADMINISTRA LOS DOCUMENTOS DE RPS

Los documentos relacionados con la presente RPS, y demás documentos normativos son administrados por Identity, y verificados por BIT4ID, cada nueva versión será presentada al INDECOPI, y luego de su aprobación, será debidamente publicada en la siguiente dirección url: **https://soluti.pe/legal**

Para mayor detalle al respecto se podrá consultar a la siguiente persona:

- Nombre: Brenda Alicia Salas Chavez
- Cargo: Responsable de la Entidad de Registro o Verificación – ER.
- Dirección de correo electrónico: brenda.salas@solutitech.com

9 RESPONSABILIDADES DE LOS TITULARES Y/O SUSCRIPTORES

Los usuarios y solicitantes de los certificados digitales provistos por Identity son responsables de revisar el presente documento, la CPS y las Políticas de Certificación de BIT4ID, a fin de tener conocimiento 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.

10 PUBLICACIÓN DE LA DECLARACIÓN DE PRÁCTICAS Y OTROS DOCUMENTOS

La Declaración de Prácticas de Registro (RPS), así como la Política de Seguridad, Política y Plan de Privacidad de la Entidad de Registro o Verificación - ER Identity, y otra documentación relevante son publicadas en la siguiente dirección:
https://soluti.pe/legal

Asimismo, la Declaración de Prácticas y Políticas de Certificación de la Entidad de Certificación – EC BIT4ID y otra documentación relevante son publicadas en la siguiente dirección:
https://www.bit4id.com/es/

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

El presente documento es firmado por el responsable de la ER Identity antes de ser publicado, comprometiéndose dicho responsable de controlar las versiones de este, 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 IDENTIFICACIÓN Y AUTENTICACIÓN

11.1 NOMBRES

11.1.1 TIPOS DE NOMBRES

La información descrita en este apartado se encuentra detallada en la Declaración de Prácticas y Políticas de Certificación de BIT4ID.

11.1.2 PSEUDÓNIMOS

La información descrita en este apartado se encuentra detallada en la Declaración de Prácticas y Políticas de Certificación de BIT4ID.

11.1.3 REGLAS UTILIZADAS PARA INTERPRETAR VARIOS FORMATOS DE NOMBRES

La información descrita en este apartado se encuentra detallada en la Declaración de Prácticas y Políticas de Certificación de BIT4ID.

11.1.4 UNICIDAD DE LOS NOMBRES

La información descrita en este apartado se encuentra detallada en la Declaración de Prácticas y Políticas de Certificación de BIT4ID.

11.1.5 RECONOCIMIENTO, AUTENTICACIÓN Y FUNCIÓN DE LAS MARCAS REGISTRADAS

La información descrita en este apartado se encuentra detallada en la Declaración de Prácticas y Políticas de Certificación de BIT4ID.

11.1.6 MÉTODOS DE PRUEBA DE LA POSESIÓN DE LA CLAVE PRIVADA

La información descrita en este apartado se encuentra detallada en la Declaración de Prácticas y Políticas de Certificación de BIT4ID.

11.1.7 AUTENTICACIÓN DE LA IDENTIDAD DE UN INDIVIDUO, LA ENTIDAD Y SU VINCULACIÓN

La información descrita en este apartado se encuentra detallada en la Declaración de Prácticas y Políticas de Certificación de BIT4ID.

12 SOLICITUD DE EMISIÓN DE CERTIFICADOS DIGITALES

Los procedimientos, requisitos de solicitud y responsabilidades en el uso de los certificados, pueden variar de acuerdo a lo establecido en la Política de Certificación y Declaración de Prácticas de BIT4ID, los mismos que son publicados en la siguiente dirección web:
https://www.bit4id.com/es/

El ciclo de vida de un certificado personal no debe exceder de Tres (03) años conforme lo estipulado por la IOFE. Los certificados que se ofrecerán son

- Certificado de persona jurídica:
    a. Certificado de Atributos, caracterizados por el hecho que el titular del certificado es una persona jurídica, que faculta a una persona natural de atributos que le permiten actuar en nombre de la persona jurídica. Dichos atributos pueden ser limitados como el caso de certificados de funcionarios o empleados, o plenos como es el caso del representante legal de la persona jurídica.
    b. . Certificados de agente automatizado,

  Cuando el poseedor de la clave privada es un dispositivo informático perteneciente a una persona jurídica que realiza las operaciones de firma y descifrado de forma automática, y cuyas acciones se encuentran bajo la responsabilidad de una persona física que es el suscriptor del certificado (Puede ser el caso de un sistema SID, PSC, Time Stamping, etc.)
- Certificado de persona natural: caracterizados por el hecho de que pertenecen a una persona física, que actúa a nombre propio y representación (siendo en este caso el suscriptor y titular del certificado la misma persona).

12.1 SOLICITUD DE CERTIFICADOS DE PERSONA JURÍDICA

12.1.1 SERVICIOS BRINDADOS POR IDENTITY

La ER brinda los siguientes servicios a personas jurídicas:

- Atención de solicitudes de emisión, revocación, suspensión y re-emisión[2] de certificados de atributos para personas jurídicas públicas o privadas, constituidas en el Perú, para ser usados por representantes legales, funcionarios y personal específico.
- Atención de solicitudes de emisión, revocación, suspensión y re-emisión[3] de certificados de atributos para personas jurídicas públicas o privadas, constituidas en el extranjero, para ser usados por representantes legales, funcionarios y personal específico.
- Atención de solicitudes de emisión, revocación, suspensión y re-emisión[4] de certificados que serán usados por agentes automatizados de personas jurídicas públicas o privadas, constituidas en el Perú, como por ejemplo, servidores de firmas de transacciones y servidores de sellado de tiempo.
- Atención de solicitudes de emisión, revocación, suspensión y re-emisión[5] de certificados que serán usados por agentes automatizados de personas jurídicas públicas o privadas, constituidas en el extranjero, como por ejemplo, servidores de firmas de transacciones y servidores de sellado de tiempo.

Los certificados brindados por la ER corresponden a BIT4ID y dicha información se encuentra publicada en la siguiente dirección:
https://www.bit4id.com/es/

12.1.2 PERSONAS AUTORIZADAS PARA REALIZAR LA SOLICITUD

En los supuestos, tanto de certificados de atributos como certificados para agentes automatizados, la solicitud debe ser hecha por un representante designado por la persona jurídica, el cual deberá presentar al Operador de Registro de la ER, la documentación legal que acredite sus facultades como representante.
Asimismo, la solicitud debe realizarse por medios o canales de no repudio, ya sea de manera presencial o virtual mediante un link cifrado y correos corporativos oficiales.

12.1.3 FORMAS DE ATENCIÓN

La solicitud deberá ser realizada mediante un contrato de adquisición de certificado digital ("Contrato de Suscriptor y Licencias de Certificados Digitales Personales", en adelante "El Contrato"), que puede ser celebrado de las siguientes formas:

- ✓ De manera presencial en las instalaciones de la ER
- ✓ De manera presencial en las instalaciones del cliente, o un lugar asignado por él en presencia de un representante de la ER
- ✓ De efectuarse de manera remota, deberá suscribirse electrónicamente el contrato de adquisición de certificado digital, con la firma digital del representante asignado por la persona jurídica.

[2] La suspensión, re-emisión y modificación dependerá de lo establecido en la CPS de la Entidad de Certificación vinculada a Identity.

[3] La suspensión, re-emisión y modificación dependerá de lo establecido en la CPS de la Entidad de Certificación vinculada a Identity.

[4] La suspensión, re-emisión y modificación dependerá de lo establecido en la CPS de la Entidad de Certificación vinculada a Identity.

[5] La suspensión, re-emisión y modificación dependerá de lo establecido en la CPS de la Entidad de Certificación vinculada a Identity.

Los documentos electrónicos serán firmados digitalmente por un Operador de Registro en la ER utilizando un certificado digital reconocido por el INDECOPI.

12.1.4 SOLICITUD DE CERTIFICADOS DE ATRIBUTOS

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 solicitante 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.

Un mismo suscriptor podrá efectuar solicitudes referentes a múltiples titulares, siempre y cuando exista entre las partes una relación de por medio que faculte al suscriptor para proceder de esa manera.

12.1.5 SOLICITUD DE CERTIFICADOS PARA AGENTES AUTOMATIZADOS

En el supuesto 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 dueña del dispositivo. En este supuesto, 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.

El propósito del certificado y el módulo criptográfico a emplear, deberá detallarse en la solicitud.

12.1.6 VIGENCIA DE LOS CERTIFICADOS

En el supuesto de los certificados de atributos, el periodo de vigencia de los certificados solicitados no deberá exceder de tres (03) años de acuerdo a la legislación vigente.

En el supuesto de certificados para agentes automatizados, el periodo de vigencia puede variar conforme a lo establecido en la Política de Certificación y Declaración de Prácticas de Certificación de la EC

12.1.7 RECONOCIMIENTO, AUTENTICACIÓN Y FUNCIÓN 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 podrá rechazar una solicitud de certificado a causa de conflicto de nombres, en vista que no se podrá volver a asignar un nombre de titular que ya haya sido asignado a un titular diferente.

A través de la verificación de la documentación e información que figura en Registros Públicos o la embajada correspondiente, la ER determinará la validez del nombre de la persona jurídica. Sin embargo, no le corresponde a ésta última, determinar si a un solicitante le asiste algún tipo de derecho sobre el nombre que figura en una solicitud de certificado, asimismo, no es competencia de la ER , la resolución de cualquier disputa concerniente a la propiedad de nombres de personas naturales o jurídicas, nombres de dominio, marcas o nombres comerciales.
en ningún caso le corresponde a la ER resolver disputas relacionadas con la propiedad de nombres de personas naturales o jurídicas, nombres de dominio, marcas o nombres comerciales.

Las disputas sobre la propiedad de estos activos intangibles son complejas ya menudo requieren un análisis legal y administrativo detallado. En su lugar, la ER se adhiere estrictamente a su papel

de verificar la identidad de los solicitantes de certificados digitales y garantizar la seguridad de los procesos de emisión y gestión de certificados.

En caso de que surja una disputa sobre la propiedad de nombres o marcas, se recomienda a las partes involucradas recurrir a los mecanismos legales y administrativos pertinentes, como los tribunales de justicia o los organismos reguladores especializados en propiedad intelectual. La ER, como entidad neutral en esta cuestión

12.1.8 IDENTIFICACIÓN Y AUTENTICACIÓN DE SOLICITANTES DE CERTIFICADOS DE PERSONA JURÍDICA

El solicitante deberá acreditar la existencia de la persona jurídica y su vigencia mediante los documentos públicos expedidos por los Registros Públicos, o mediante la especificación de la norma legal de creación de la persona jurídica correspondiente. La información brindada por los solicitantes será validada a través de la consulta a la Superintendencia Nacional de los Registros Públicos (SUNARP). Además, es necesario verificar la situación tributaria de la entidad a través de la base de datos de la Superintendencia Nacional de Aduanas y de Administración Tributaria (SUNAT), asegurando que el Registro Único de Contribuyentes (RUC) se encuentre activo y en estado de "habido".

Estos procedimientos garantizan la validez y legalidad de las entidades jurídicas en el ámbito peruano, proporcionando una base sólida para la emisión y gestión de certificados digitales dentro del marco normativo establecido.

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.

12.1.9 CONTRATO DE SUSCRIPTOR

.

La Entidad de Registro (ER) cuenta con una póliza de responsabilidad que garantiza la seguridad de la información proporcionada por los titulares. El acuerdo del suscriptor debe contemplar las obligaciones cuando la legislación así lo establece para los suscriptores o titulares, con el fin de asegurar los efectos legales de las transacciones realizadas utilizando certificados emitidos por la Entidad Certificadora (EC).

El representante legal de la persona jurídica o una persona asignada por él, debidamente acreditada a través de una declaración jurada, deberá firmar 'El Contrato'. Mediante este documento, el titular y/o suscriptor declarará tener pleno conocimiento de los términos y condiciones aplicables a los certificados. La celebración de dicho contrato deberá realizarse antes de la emisión de los certificados.

Cuando un suscriptor firma un acuerdo en nombre de varios titulares, es fundamental que las responsabilidades del suscriptor con respecto a las acciones de esos titulares estén claramente definidas.

En el contrato de una persona jurídica, es vital diferenciar entre el titular y el suscriptor. La diferencia radica en sus roles y responsabilidades dentro del proceso de certificación digital:

- Titular: Se refiere a la entidad misma, es decir, la empresa u organización que posee el certificado digital. El titular es quien ejerce los derechos y recibe los beneficios derivados del certificado, como la capacidad de realizar transacciones digitales en nombre de la organización.
- Suscriptor: Suelen ser representantes legales designados por la persona jurídica para actuar en su nombre en el proceso de certificación. El suscriptor firma el contrato de certificación en

nombre de la persona jurídica y asume las responsabilidades asociadas con la obtención y el uso del certificado digital. Además, puede ser responsable de solicitar y gestionar el certificado en nombre de la entidad.

Es fundamental incluir la responsabilidad de los titulares y suscriptores de solicitar la revocación del certificado en caso de tomar conocimiento de cualquiera de las siguientes circunstancias:

- Por exposición, puesta en peligro o uso indebido de la clave privada.
- Por deterioro, alteraciones o cualquier otro hecho u acto que afecte la clave privada.
- Revocación de las facultades de representación y/o poderes de sus representantes legales o apoderados.
- Cuando la información contenida en el certificado ya no resulta correcta.
- Cuando el suscriptor deja de ser miembro de la comunidad de interés o se sustrae de aquellos intereses relativos a la Entidad Certificadora (EC).
- Cuando el suscriptor o titular incumple las obligaciones a las que se encuentra comprometida dentro de la Infraestructura de Firma Electrónica (IOFE) según lo estipulado en el contrato del suscriptor y/o titular.
- Por decisión de la legislación respectiva.

Estas disposiciones aseguran que los titulares y suscriptores asuman la responsabilidad de mantener la integridad y la seguridad del certificado digital, así como de cumplir con las obligaciones y regulaciones pertinentes en el uso de la firma electrónica.El titular puede enviar un correo para solicitar la revocación de su certificado tanto a la EC como a la ER. También se le facilita enviar su usuario para recibir un código ERC. En ese correo de comunicación, se le comparte un enlace para anular o revocar el certificado, indicando debidamente sus motivos.

12.1.10 VERIFICACIÓN DEL SUSCRIPTOR

Los solicitantes de un certificado digital deben ser validados de acuerdo con los siguientes métodos:

- Presencialmente en las instalaciones de la Entidad Registradora (ER).
- Presencialmente en las instalaciones del cliente, o en un lugar designado por él, en presencia de un representante de la ER. En ambos casos, el representante de la ER verificará la identidad del titular mediante la consulta del Registro Nacional de Identificación y Estado Civil (RENIEC) utilizando su Documento Nacional de Identidad (DNI). Además, se tomará una fotografía del titular junto a la primera cara de su DNI como evidencia de la validación exitosa.
- De manera remota, a través de un correo electrónico enviado al titular. Al acceder al correo, el titular seleccionará la opción para tomar una fotografía, lo que abrirá la cámara de su dispositivo. A continuación, se tomará una selfie mostrando la primera cara de su DNI vigente.

Para verificar la identidad de los solicitantes, se deben cumplir los requisitos establecidos en el presente documento con respecto a la autenticación de personas 15urídicas

Cuando una persona solicite la emisión de un certificado digital para demostrar el ejercicio de un cargo específico, la ER requerirá al solicitante la documentación legal que respalde dicho cargo, incluyendo las facultades para realizar el proceso solicitado. Además, el solicitante debe presentar el original de su propio documento oficial de identidad.

12.2 SOLICITUD DE CERTIFICADOS DE PERSONA NATURAL

12.2.1 SERVICIOS BRINDADOS POR IDENTITY

La ER brinda los siguientes servicios a personas naturales:

- Atención de solicitudes de emisión, revocación, suspensión, re-emisión y modificación[6] de certificados para personas naturales de nacionalidad peruana.
- Atención de solicitudes de emisión, revocación, suspensión, re-emisión y modificación[7] de certificados de atributos para personas naturales de nacionalidad extranjera.
-

Los certificados digitales se solicitan a través de medios no repudiables, ya sea de manera presencial o virtual mediante un link cifrado para el ingreso de la solicitud y son emitidos por la Entidad de Certificación BIT4ID.

12.2.2 PERSONA AUTORIZADA PARA REALIZAR LA SOLICITUD

En el caso de personas naturales, la solicitud deberá ser hecha por la misma persona que pretende ser titular del certificado digital.

12.2.3 FORMAS DE ATENCIÓN

La solicitud deberá ser realizada mediante "El Contrato" que puede ser celebrado de las siguientes formas:

- ✓ De manera presencial en las instalaciones de la ER.
- ✓ De manera presencial en las instalaciones del cliente, o un lugar asignado por él en presencia de un representante de la ER.
- ✓ De efectuarse de manera remota, deberá suscribirse electrónicamente el contrato de adquisición de certificado digital, con la firma digital del representante asignado por la persona jurídica.

Los documentos electrónicos serán firmados digitalmente por un Operador de Registro de la ER utilizando un certificado digital reconocido por el INDECOPI.

De esta manera, consideramos que los medios presentados garantizan el no repudio. Asimismo, las computadoras utilizadas por el Operador de Registro deberá tener una aplicación antivirus y los parches del sistema de antivirus actualizados

12.2.4 SOLICITUD DE CERTIFICADOS DE PERSONA NATURAL

El solicitante podrá realizar su solicitud a través de cualquiera de las modalidades de atención descritas en el presente documento, portando el original de su documento nacional de identidad, el mismo que debe estar vigente a la fecha de realización del proceso de registro.

12.2.5 CONTRATO DE SUSCRIPTOR

El solicitante está obligado a firmar "El Contrato", en el cual se especifican las obligaciones que deben cumplir los suscriptores y titulares de un certificado digital, de conformidad con la legislación especial para garantizar de esta manera el efecto legal de las transacciones realizadas, así como sus consecuencias en el supuesto de no cumplir con dicho acuerdo.

---

[6] La suspensión, re-emisión y modificación dependerá de lo establecido en la CPS de la Entidad de Certificación vinculada a Identity.

[7] La suspensión, re-emisión y modificación dependerá de lo establecido en la CPS de la Entidad de Certificación vinculada a Identity

Este documento deberá ser firmado de manera manuscrita o digital, teniendo la ER la obligación de archivarlo en un lugar seguro, bajo su custodia.

A través de dicho acuerdo, el suscriptor declara conocer los términos y condiciones aplicables a los certificados digitales. Su celebración deberá realizarse antes de la emisión del certificado digital.
Si el contrato se envía de forma virtual, se le enviará al destinatario un correo electrónico cifrado con el enlace al contrato. Antes de proceder a la firma, el destinatario deberá ingresar al enlace y colocar un token de seguridad, el cual será enviado al titular por mensaje de texto y correo electrónico. Una vez que se haya ingresado el token, se permitirá al destinatario firmar el contrato de manera electronica.
La Entidad de Registro (ER) cuenta con una póliza de responsabilidad que garantiza la seguridad de la información proporcionada por los titulares. El acuerdo del suscriptor debe contemplar las obligaciones cuando la legislación así lo establece para los suscriptores o titulares, con el fin de asegurar los efectos legales de las transacciones realizadas utilizando certificados emitidos por la Entidad Certificadora (EC).

El titular y/o suscriptor declarará tener pleno conocimiento de los términos y condiciones aplicables a los certificados. La celebración de dicho contrato deberá realizarse antes de la emisión de los certificados.

Es fundamental incluir la responsabilidad de los titulares de solicitar la revocación del certificado en caso de tomar conocimiento de cualquiera de las siguientes circunstancias:

- Por exposición, puesta en peligro o uso indebido de la clave privada.
- Por deterioro, alteraciones o cualquier otro hecho u acto que afecte la clave privada.
- Revocación de las facultades de representación y/o poderes de sus representantes legales o apoderados.
- Cuando la información contenida en el certificado ya no resulta correcta.
- Cuando el suscriptor deja de ser miembro de la comunidad de interés o se sustrae de aquellos intereses relativos a la Entidad Certificadora (EC).
- Cuando el suscriptor o titular incumple las obligaciones a las que se encuentra comprometida dentro de la Infraestructura de Firma Electrónica (IOFE) según lo estipulado en el contrato del suscriptor y/o titular.
- Por decisión de la legislación respectiva.

Estas disposiciones aseguran que los titulares asuman la responsabilidad de mantener la integridad y la seguridad del certificado digital, así como de cumplir con las obligaciones y regulaciones pertinentes en el uso de la firma electrónica.
El titular puede enviar un correo para solicitar la revocación de su certificado tanto a la EC como a la ER. También se le facilita enviar su usuario para recibir un código ERC. En ese correo de comunicación, se le comparte un enlace para anular o revocar el certificado, indicando debidamente sus motivos.

12.2.6 VERIFICACIÓN DEL SUSCRIPTOR

Los solicitantes de un certificado digital deben ser validados de acuerdo con los siguientes métodos:

- Presencialmente en las instalaciones de la Entidad Registradora (ER).

 Presencialmente en las instalaciones del cliente, o en un lugar designado por él, en presencia de un representante de la ER. En ambos casos, el representante de la ER verificará la identidad del titular mediante la consulta del Registro Nacional de Identificación y Estado Civil (RENIEC) utilizando su Documento Nacional de Identidad (DNI). Además, se tomará una fotografía del titular junto a la primera cara de su DNI como evidencia de la validación exitosa.
 De manera remota, a través de un correo electrónico enviado al titular. Al acceder al correo, el titular seleccionará la opción para tomar una fotografía, lo que abrirá la cámara de su dispositivo. A continuación, se tomará una selfie mostrando la primera cara de su DNI vigente.
Para verificar la identidad de los solicitantes, se deben cumplir los requisitos establecidos en el presente documento con respecto a la autenticación de personas juridicas

Cuando una persona solicite la emisión de un certificado digital para demostrar el ejercicio de un cargo específico, la ER requerirá al solicitante la documentación legal que respalde dicho cargo, incluyendo las facultades para realizar el proceso solicitado. Además, el solicitante debe presentar el original de su propio documento oficial de identidad.

12.2.7 VIGENCIA DE LOS CERTIFICADOS

En el caso de los certificados de personas naturales, la vigencia de los certificados solicitados no deberá exceder el periodo de tres (3) años de acuerdo a la legislación vigente.

12.2.8 IDENTIFICACIÓN Y AUTENTICACIÓN DE SOLICITANTES DE CERTIFICADOS DE PERSONA NATURAL

Identity, en su calidad de Entidad de Registro o Verificación, a través de accesos personales de sus operadores de registro, consulta a las bases de datos del RENIEC, que la información proporcionada por los solicitantes de nacionalidad peruana sea válida.

En el caso de personas naturales de nacionalidad extranjera, se acreditará su existencia y vigencia mediante su carnet de extranjería.

Conforme a lo dispuesto por la IOFE, de forma genérica no se incluirá en los certificados, información no verificada del suscriptor o el titular, según sea el caso. Salvo la única excepción de la dirección de correo electrónico del suscriptor. En este caso, los operadores de registro de la ER verificarán que la dirección de correo electrónico que se incluye en el certificado es la que efectivamente desea incluir el solicitante.

La ER no asumirá la responsabilidad de verificar lo siguiente:
- La existencia de la cuenta de correo electrónico indicada por el solicitante.
- Que la dirección sea única.
- El correcto funcionamiento del correo electrónico.

Todo lo descrito, es responsabilidad del solicitante.

13 PROCESAMIENTO DE LA SOLICITUD

13.1 RECHAZO DE LA SOLICITUD DE EMISION DE UN CERTIFICADO

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

- ✓ En el caso de personas naturales, tener plena capacidad de ejercicio de sus derechos civiles.
- ✓ En el caso de personas jurídicas, acreditar la existencia de la persona jurídica y su vigencia mediante los documentos públicos o norma legal respectiva, debiendo contar con un representante debidamente acreditado para tales efectos.

Así como en el supuesto que, el resultado de la validación realizada por la ER fuese negativo, conforme a lo establecido en este documento.

Identity, en su calidad de Entidad de Registro o Verificación, tiene la facultad de establecer en su RPS u otra documentación relevante, circunstancias adicionales para el rechazo de la solicitud, asumiendo las consecuencias que podría acarrear tal decisión.

13.2 APROBACIÓN DE LA SOLICITUD DE EMISIÓN DE UN CERTIFICADO

Para aprobar una solicitud, la ER realizará lo siguiente:

- Comunicar a la EC su aprobación para le emisión del certificado, a través de un sistema web con control de acceso, y la protección de un canal SSL. Este sistema será brindado por la EC.
- Será necesaria la firma del "El Contrato".

13.3 REGISTRO DE DOCUMENTOS

La ER registrará y archivará la solicitud, "El Contrato", y demás documentación legal presentada 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 debe realizarse bajo presencia y responsabilidad no transferible del suscriptor. En caso de realizarse la generación de claves fuera de las instalaciones de la ER, la petición PKCS#10 debe realizarse a través de medios de comunicación no repudiables, de modo que no pueda ocurrir una suplantación de la petición PKCS#10.

Los módulos criptográficos distribuidos y proporcionados por BIT4ID cuentan con la certificación FIPS 140-2 o equivalente. Es señalar preciso que únicamente el suscriptor deberá conocer las claves de acceso al módulo criptográfico donde se realiza la generación de la clave.

Posteriormente, se realizará la petición segura del certificado a la respectiva EC en el formato PKCS#10, realizando con ello la prueba de la posesión de la clave privada

13.5 TIEMPO PARA EL PROCESAMIENTO DE LA SOLICITUD DE UN CERTIFICADO

Cuando la información ha sido validada y aprobada por un operador de registro de la ER, ésta enviará a BIT4ID la autorización de la emisión del certificado, inmediatamente.

El máximo tiempo de respuesta para la emisión del certificado será de 03 días, luego de haber sido aprobada la validación de identidad y de la verificación del pago respectivo, en la cuenta bancaria de Identity, por el servicio brindado.

13.6 EMISIÓN DEL CERTIFICADO

La emisión del certificado será realizada virtualmente, vale decir a través del correo electrónico proporcionado por el suscriptor en su solicitud.

14 SOLICITUD DE RE-EMISIÓN DE CERTIFICADOS DIGITALES

La re-emisión de un certificado es un proceso programado cada vez que un nuevo par de claves debe ser emitido, debido a que la fecha de su expiración es cercana y su periodo de vigencia es menor a un plazo máximo de un año. En el supuesto que un certificado del titular hubiera expirado o hubiera sido revocado, deberá seguirse el proceso de solicitud para la emisión de un nuevo certificado, conforme se describe en éste documento.

Cabe señalar, que se podrá realizar una única re-emisión de certificado. Los procedimientos, requisitos de solicitud y responsabilidades en el uso de los certificados, pueden variar de acuerdo con lo establecido en la Política de Certificación y Declaración de Prácticas de la EC BIT4ID, a la que la ER Identity se encuentra vinculada, para cada tipo de certificado.
La reemisión del certificado solo puede llevarse a cabo una vez para certificados cuya fecha de vencimiento sea menor o igual a un año antes de cumplirse el período de vigencia. Además, el certificado reemitido debe tener un período de vigencia máximo de un año. Esta restricción garantiza que la reemisión del certificado se realiza de manera controlada y limitada, y que el nuevo certificado emitido mantiene un período de vigencia coherente con el tiempo restante de validez del certificado original. De esta manera, se asegura la adecuada gestión y renovación de los certificados digitales, manteniendo la seguridad y la integridad de los procesos de certificaciónveri

Conforme a lo establecido en legislación especial, la ER realizará como mínimo, los siguientes procedimientos de verificación para la validación de la identidad de una persona jurídica o natural:

14.1 SOLICITUD DE RE-EMISIÓN DE UN CERTIFICADO DE PERSONA JURÍDICA

14.1.1 SERVICIOS BRINDADOS POR IDENTITY

La ER brinda los siguientes servicios a personas jurídicas:

- Atención de solicitudes de re-emisión[8] de certificados de atributos para personas jurídicas públicas o privadas, constituidas en el Perú, para ser usados por representantes legales, funcionarios y personal específico.
- Atención de solicitudes de re-emisión[9] de certificados de atributos para personas jurídicas públicas o privadas, constituidas en el extranjero, para ser usados por representantes legales, funcionarios y personal específico.
- Atención de solicitudes de re-emisión de certificados que serán usados por agentes automatizados de personas jurídicas públicas o privadas, constituidas en el Perú, como por ejemplo, servidores de firmas de transacciones y servidores de sellado de tiempo.
- Atención de solicitudes de re-emisión de certificados que serán usados por agentes automatizados de personas jurídicas públicas o privadas, constituidas en el extranjero, como por ejemplo, servidores de firmas de transacciones y servidores de sellado de tiempo.

Los certificados digitales son emitidos por la Entidad de Certificación BIT4ID.
Los solicitantes de un certificado digital deben ser validados de acuerdo con los siguientes métodos:

- Presencialmente en las instalaciones de la Entidad Registradora (ER).
- Presencialmente en las instalaciones del cliente, o en un lugar designado por él, en presencia de un representante de la ER. En ambos casos, el representante de la ER verificará la identidad del titular mediante la consulta del Registro Nacional de Identificación y Estado Civil (RENIEC) utilizando su Documento Nacional de Identidad (DNI). Además, se tomará una fotografía del titular junto a la primera cara de su DNI como evidencia de la validación exitosa.
- De manera remota, a través de un correo electrónico enviado al titular. Al acceder al correo, el titular seleccionará la opción para tomar una fotografía, lo que abrirá la cámara de su dispositivo. A continuación, se tomará una selfie mostrando la primera cara de su DNI vigente.

Para verificar la identidad de los solicitantes, se deben cumplir los requisitos establecidos en el presente documento con respecto a la autenticación de personas naturales.

[8] La suspensión, re-emisión y modificación dependerá de lo establecido en la CPS de la Entidad de Certificación vinculada a Identity

[9] La suspensión, re-emisión y modificación dependerá de lo establecido en la CPS de la Entidad de Certificación vinculada a Identity

Previamente el encargado de la ER pedirá documentación como el DNI vigente, la ficha ruc en mes en curso así como la vigencia de poder con facultades contractuales, de no tener facultades, se le facilitará un formato de autorización para que lo firme una persona con facultades contractuales verificando que sea así con la vigencia de poder y DNI del que autoriza.

Cuando una persona solicite la emisión de un certificado digital para demostrar el ejercicio de un cargo específico, la ER requerirá al solicitante la documentación legal que respalde dicho cargo, incluyendo las facultades para realizar el proceso solicitado. Además, el solicitante debe presentar el original de su propio documento oficial de identidad.

14.1.2 PERSONAS AUTORIZADAS PARA REALIZAR LA SOLICITUD

Únicamente los titulares de certificados pueden solicitar la re-emisión de certificados, en consecuencia, en los supuestos de certificados de atributos, así como certificados para agentes automatizados, la solicitud debe ser hecha por un representante designado por la persona jurídica, el cual deberá presentar al Operador de Registro de la ER, la documentación legal que acredite sus facultades como representante.

Si como parte de la solicitud inicial el representante ya ha sido validado y registrado por la ER, bastará con presentar su solicitud firmada de manera manuscrita o con firma digital al Operador de Registro. En el caso de que la solicitud sea firmada de manera manuscrita, el solicitante deberá presentar su documento oficial de identidad.

14.1.3 FORMAS DE ATENCIÓN

La solicitud deberá ser realizada mediante un contrato de adquisición de certificado digital que puede ser celebrado de las siguientes formas:

- ✓ De manera presencial en las instalaciones de la ER.
- ✓ De manera presencial en las instalaciones del cliente, o un lugar asignado por él en presencia de un representante de la ER.
- ✓ De efectuarse de manera remota, deberá suscribirse electrónicamente el contrato de adquisición de certificado digital, con la firma digital del representante asignado por la persona jurídica.

Los documentos electrónicos serán firmados digitalmente por un Operador de Registro de la ER utilizando un certificado digital reconocido por el INDECOPI.

14.1.4 SOLICITUD DE RE-EMISIÓN DE CERTIFICADOS DE ATRIBUTOS

El solicitante 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.

14.1.5 SOLICITUD DE RE-EMISIÓN DE CERTIFICADOS PARA AGENTES AUTOMATIZADOS

En el supuesto 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 propietaria del dispositivo. En dicha solicitud deberá especificarse el propósito del certificado y el módulo criptográfico a emplear.

14.1.6 IDENTIFICACIÓN Y AUTENTICACIÓN DE SOLICITANTES DE RE-EMISIÓN DE CERTIFICADOS DE PERSONA JURÍDICA

La ER verificará que la información del titular y/o suscriptor contenida en la solicitud continúa siendo válida, respecto de la existencia de la persona jurídica en los Registros Públicos y SUNAT; y de los suscriptores en la base de datos del RENIEC.

En el caso que cualquier información del titular y/o del suscriptor hubiere cambiado, se registrará adecuadamente la nueva información. En este caso el titular o su representante deben presentar la documentación legal, que respalde dichas modificaciones.

En el caso de empresas constituidas en el extranjero, el solicitante deberá acreditar la continuidad de su existencia y vigencia mediante un certificado de vigencia de la sociedad u otro documento equivalente expedido por la autoridad competente en su país de origen.

En el caso de suscriptores extranjeros, estos tendrán que presentar al Operador de Registro, su documento oficial de identidad, pasaporte o carnet de extranjería, según sea el caso.

14.2 SOLICITUD DE RE-EMISIÓN DE CERTIFICADOS DE PERSONA NATURAL

14.2.1 SERVICIOS BRINDADOS POR IDENTITY

La ER brinda los siguientes servicios a personas naturales:

- Atención de solicitudes de re-emisión[10] de certificados de atributos para personas naturales de nacionalidad peruana.
- Atención de solicitudes de re-emisión[11] de certificados de atributos para personas naturales de nacionalidad extranjera

Los certificados digitales son emitidos por la Entidad de Certificación BIT4ID.
Asimismo, la solicitud se realiza a través de correo electrónico, medio no repudiable, del titular; De esta manera, los suscriptores expresan su conformidad respecto a la re-emision del certificado y las responsabilidades implicadas

Por último, como ER nos aseguramos de que los datos de la solicitud del certificado que se envían a la EC para la emisión del certificado coincidan con los datos de la identidad validada. Con el fin de prevenir la suplantación de identidad, es necesario verificar que los datos incluidos en la solicitud PKCS#10 se correspondan con la identidad validada.

14.2.2 PERSONA AUTORIZADA PARA REALIZAR LA SOLICITUD

En este supuesto de personas naturales, la solicitud debe ser realizada por la misma persona que pretende ser titular del certificado.

14.2.3 FORMAS DE ATENCIÓN

La solicitud deberá ser realizada mediante "El Contrato" que puede ser celebrado de las siguientes formas:

- ✓ De manera presencial en las instalaciones de la ER.
- ✓ De manera presencial en alguna locación señalada por el cliente, en presencia de un representante de la ER.
- ✓ De efectuarse de manera remota, deberá suscribirse electrónicamente el contrato de adquisición de certificado digital, con la firma digital del titular y suscriptor del certificado.

[10] La suspensión, re-emisión y modificación dependerá de lo establecido en la CPS de la Entidad de Certificación vinculada a Identity

[11] La suspensión, re-emisión y modificación dependerá de lo establecido en la CPS de la Entidad de Certificación vinculada a Identity

Los documentos electrónicos serán firmados digitalmente por un Operador de Registro en la ER utilizando un certificado digital reconocido por el INDECOPI.

14.2.4 SOLICITUD DE CERTIFICADOS DE PERSONA NATURAL

Queda a elección del solicitante, realizar su solicitud bajo cualquiera de las formas de atención especificadas en el presente documento.

14.2.5 IDENTIFICACIÓN Y AUTENTICACIÓN DE SOLICITANTES DE CERTIFICADOS DE PERSONA NATURAL

La ER verificará que la información proporcionada por un solicitante de nacionalidad peruana sea válida, a través de sus accesos en la base de datos del RENIEC.

En el caso de personas naturales de nacionalidad extranjera, se acreditará su existencia y vigencia mediante su pasaporte o carnet de extranjería.

Conforme a lo dispuesto por la IOFE, de forma genérica no se incluirá en los certificados, información no verificada del suscriptor o el titular, según sea el caso. Salvo la única excepción de la dirección de correo electrónico del suscriptor. En este caso, los operadores de registro de la ER verificarán que la dirección de correo electrónico que se incluye en el certificado es la que efectivamente desea incluir el solicitante.

Si cualquier información del titular o del suscriptor hubiese cambiado, se registrara correctamente la nueva información, previa presentación de documentación que respalde dichos cambios.

15 PROCESAMIENTO DE LA SOLICITUD DE RE-EMISIÓN

15.1 RECHAZO DE UNA SOLICITUD DE RE-EMISIÓN DE UN CERTIFICADO

Una solicitud de emisión será rechazada por la ER, si el solicitante no está capacitado para participar de la comunidad de usuarios de la IOFE:

- ✓ Tratándose de personas naturales, tener plena capacidad de ejercicio de sus derechos civiles.
- ✓ Tratándose de personas jurídicas, acreditar la existencia de la persona jurídica y su vigencia mediante la documentación legal necesaria, 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.

La EC BIT4ID 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.

15.2 APROBACIÓN DE LA SOLICITUD DE EMISIÓN DE UN CERTIFICADO

A fin de que una solicitud sea aprobada, la ER realizará lo siguiente:

- ✓ Comunicar a la EC su aprobación para la emisión del certificado mediante un sistema web con control de acceso y la protección de un canal SSL. Este sistema será brindado por BIT4ID.
- ✓ Se requerirá la firma del contrato del suscriptor.

15.3 REGISTRO DE DOCUMENTOS

La ER tiene la obligación de registrar y archivar la solicitud, el “Acuerdo del Suscriptor”, 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.

15.4 MÉTODO PARA PROBAR LA POSESIÓN DE LA CLAVE PRIVADA

La generación del par de claves debe realizarse bajo presencia y responsabilidad no transferible del suscriptor. En caso de realizarse la generación de claves fuera de las instalaciones de la ER, la petición PKCS#10 debe realizarse a través de medios de comunicación no repudiables, de modo que no pueda ocurrir una suplantación de la petición PKCS#10.

Los módulos criptográficos distribuidos y proporcionados por BIT4ID cuentan con la certificación FIPS 140-2 o equivalente. Es señalar preciso que únicamente el suscriptor deberá conocer las claves de acceso al módulo criptográfico donde se realiza la generación de la clave.

Posteriormente, se realizará la publión segura del certificado a la respectiva EC en el formato PKCS#10, realizando con ello la prueba de la posesión de la clave privada

15.5 TIEMPO PARA EL PROCESAMIENTO DE LA SOLICITUD DE UN CERTIFICADO

Cuando la información ha sido validada y aprobada por un operador de registro de la ER, ésta enviará a la respectiva EC la autorización de la emisión del certificado, inmediatamente.

El máximo tiempo de respuesta para la emisión del certificado será de 03 días, luego de haber sido aprobada la validación de identidad y de la verificación del pago respectivo, en la cuenta bancaria de Identity, por el servicio brindado.

15.6 RE-EMISIÓN DEL CERTIFICADO

La re-emisión del certificado será realizada virtualmente, vale decir a través del correo electrónico proporcionado por el suscriptor en su solicitud, considerando este como un medio no repudiable

16 SOLICITUD DE REVOCACIÓN DE CERTIFICADOS

16.1 SITUACIONES PARA REALIZAR LA SOLICITUD

A efectos de una solicitud de revocación, el titular y suscriptor de un certificado digital, bajo su responsabilidad, pueden realizar la mencionada solicitud, al tener conocimiento de la ocurrencia de cualquiera de las siguientes situaciones:

- ✓ Por exposición, puesta en peligro o uso indebido de la clave privada.
- ✓ Por deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada.
- ✓ Revocación de las facultades de representación y/o poderes de los representantes legales o apoderados de la persona jurídica privada o pública.
- ✓ Cuando la información contenida en el certificado ya no resulte correcta.
- ✓ Cuando el suscriptor deja de ser miembro de la comunidad de interés o se sustrae de aquellos intereses relativos a la EC.
- ✓ Cuando el suscriptor o titular incumple las obligaciones a las que se encuentra comprometido dentro de la IOFE, a través de lo estipulado en el “Acuerdo del Suscriptor”.
- ✓ Por decisión de la legislación respectiva.
- ✓ Por resolución administrativa o judicial que lo ordene.
  El titular puede enviar un correo para solicitar la revocación de su certificado tanto a la EC como a la ER. También se le facilita enviar su usuario para recibir un código ERC. En ese correo de comunicación, se le comparte un enlace para anular o revocar el certificado, indicando debidamente sus motivos.

16.2 SOLICITUD DE REVOCACIÓN DE CERTIFICADOS

16.2.1 SERVICIOS BRINDADOS POR IDENTITY

La ER brinda los siguientes servicios a personas jurídicas y naturales:

- Atención de solicitudes de revocación de certificados para personas naturales de nacionalidad peruana.
- Atención de solicitudes de revocación de certificados de atributos para personas naturales de nacionalidad extranjera.
- Atención de solicitudes de revocación de certificados de atributos para personas jurídicas públicas o privadas, constituidas en el Perú, para ser usados por representantes legales, funcionarios y personal específico.
- Atención de solicitudes de revocación de certificados de atributos para personas jurídicas privadas o públicas, constituidas en el extranjero.
- Atención de solicitudes de revocación de certificados que serán usados por agentes automatizados de personas jurídicas públicas o privadas, constituidas en el Perú, como por ejemplo, servidores de firmas de transacciones y servidores de sellado de tiempo.
- Atención de solicitudes de revocación de certificados que serán usados por agentes automatizados de personas jurídicas públicas o privadas, constituidas en el extranjero, como por ejemplo, servidores de firmas de transacciones y servidores de sellado de tiempo.

Los certificados digitales provienen de la Entidad de Certificación BIT4ID.

16.2.2 PERSONAS AUTORIZADAS PARA REALIZAR LA SOLICITUD

Conforme a lo establecido por la Ley, el tipo de personas que pueden solicitar la revocación de un certificado son las siguientes:

- ✓ El titular del certificado.
- ✓ El suscriptor del certificado.
- ✓ La EC o ER que emitió el certificado.
- ✓ Un Juez que conforme a Ley decida revocar el certificado.
- ✓ Un tercero que tenga pruebas fehacientes del uso indebido del certificado, el compromiso de la clave u otro motivo de revocación mencionado en la Ley, los reglamentos de acreditación y el presente documento.

En el caso de personas jurídicas, los titulares de certificados pueden solicitar la re-emisión de certificados, por lo que la solicitud debe ser hecha por un representante designado por la persona jurídica, el cual deberá presentar al Operador de Registro de la ER, un documento que acredite sus facultades como representante.

En el supuesto que como parte de la solicitud inicial el representante ya ha sido validado y registrado por la ER, será suficiente con presentar su solicitud firmada de forma manuscrita (previa presentación de su documento oficial de identidad) o con firma digital al operador de registro.

16.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS SOLICITANTES

En el supuesto que la solicitud sea presencial:

- ✓ Los suscriptores deben demostrar su documento oficial de identidad.
- ✓ El representante legal de la persona jurídica debe presentar la documentación que acredite su representación.
- ✓ Los terceros (diferentes de la EC, el suscriptor y el titular), deberán presentar pruebas fehacientes a la ER, del uso indebido del certificado, conforme a lo estipulado por la Ley, junto a la orden judicial respectiva.

16.2.4 FORMAS DE ATENCIÓN

La solicitud deberá ser realizada por los titulares y suscriptores de las siguientes formas:

- ✓ De manera presencial en las instalaciones de la ER.
- ✓ De manera presencial en alguna locación señalada por estos, en presencia de un representante de la ER.
- ✓ De efectuarse de manera remota, mediante documento o correo electrónico firmado digitalmente por el representante legal de la persona jurídica o por el suscriptor. El certificado digital a emplear no debe ser el que se desea revocar.
- ✓ De manera remota en una comunicación directa con la EC, mediante un control de acceso o contraseña brindados al suscriptor en el momento de la solicitud de emisión del certificado.

Los demás actores, diferentes a los suscriptores y titulares, deberán realizar la solicitud de manera presencial en las instalaciones de la ER.

La EC no requerirá efectuar la solicitud a la ER en los casos que el suscriptor haya infringido las obligaciones descritas en su contrato, o en caso sea necesario por revocación del certificado de la EC. Una EC puede revocar los certificados que ha emitido, siempre y cuando los motivos de revocación estén determinados en su CPS y se encuentren conforme a la Ley.

Los documentos electrónicos serán firmados digitalmente por un Operador de Registro de la ER, utilizando un certificado digital reconocido por el INDECOPI.

16.2.5 SOLICITUD DE REVOCACIÓN DE CERTIFICADOS DE ATRIBUTOS

El solicitante 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.

16.2.6 SOLICITUD DE REVOCACIÓN DE CERTIFICADOS PARA AGENTES AUTOMATIZADOS

El solicitante 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.

16.2.7 SOLICITUD DE REVOCACIÓN DE CERTIFICADOS DE PERSONA NATURAL

El solicitante deberá realizar su solicitud en cualquiera de las modalidades de atención especificadas en el presente documento.

17. PROCESAMIENTO DE LA SOLICITUD DE REVOCACIÓN

17.1 RECHAZO DE LA SOLICITUD DE REVOCACIÓN

La solicitud de revocación de certificado será rechazada en caso no se cumpla con alguna de las formas 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:

- ✓ Tratándose de personas naturales, tener plena capacidad de ejercicio de sus derechos civiles.

- ✓ Tratándose de personas jurídicas, acreditar la existencia de la persona jurídica y su vigencia mediante los documentos legales respectivos, 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 el presente 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.

17.2 APROBACIÓN DE LA SOLICITUD DE REVOCACIÓN

Para que la ER apruebe una solicitud de revocación, se deberá cumplir con lo siguiente:

- ✓ Comunicar a la EC su aprobación para la revocación del certificado mediante un sistema web con control de acceso y la protección de un canal SSL. Este sistema será brindado por BIT4ID.
- ✓ Una copia de dicha solicitud firmada será enviada a la EC o almacenada por la ER, teniendo en cuenta su vinculación.

17.3 REGISTRO DE DOCUMENTOS

La ER registrará y archivará la solicitud 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, fecha y hora de la revocación y de la notificación de esta BIT4ID, sus suscriptores y los terceros que confían.

En cumplimiento de la Política de Seguridad de la ER, toda la documentación será protegida contra acceso no autorizado y destrucción.

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

17.4 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 comunicará a BIT4ID, por vía electrónica la revocación del certificado de manera inmediata.

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

17.5 REVOCACIÓN DEL CERTIFICADO

La revocación del certificado será comunicada al suscriptor y titular mediante el correo electrónico del suscriptor, registrado en su solicitud.

18. CONTROLES DE LAS INSTALACIONES, DE LA GESTIÓN Y CONTROLES OPERACIONALES

De acuerdo a los lineamientos establecidos por el INDECOPI, la presente sección describe de forma genérica las medidas que ha implementado Identity, en su calidad de ER, con la finalidad de garantizar los requerimientos que, en materia de seguridad, sostienen los servicios de registro o verificación de datos. El detalle de las medidas de seguridad adoptadas para proteger los activos críticos que sostienen los mencionados servicios, están establecidas en la Política de Seguridad de la ER.

En las sub secciones siguientes se reseña las medidas adoptadas más relevantes:

18.1 CONTROLES FISICOS

En esta subsección se describen los controles que se aplicarán a los recursos físicos que comprenden las instalaciones de la ER, lo cual incluye la infraestructura física y su acondicionamiento, el acceso físico a ésta, así como su protección y seguridad.

18.1.1 UBICACIÓN Y CONSTRUCCIÓN DEL LOCAL

Las instalaciones de la ER se encuentran resguardadas físicamente con las medidas de protección necesarias para salvaguardar el desarrollo de las actividades de prestación de servicios como ER.

18.1.2 ACCESO FÍSICO

En los ambientes donde se desarrollan las actividades y operaciones de la ER se han establecido perímetros de seguridad e implementado controles de acceso, de modo que solo el personal autorizado y acreditado puede acceder a los mismos. Estos controles de acceso aplican para el personal de la ER, visitantes o proveedores.

18.1.3 ENERGÍA Y AIRE ACONDICIONADO

Las instalaciones donde se encuentran los servidores que brindan soporte a las operaciones de la ER cuenta con un equipo de apoyo que suministra energía temporal en caso de caídas del sistema eléctrico principal, protegiendo a los equipos frente a fluctuaciones eléctricas que los pudieran dañar.

El ambiente donde se encuentran situados los equipos de tratamiento y almacenamiento de información, dispone de un sistema de aire acondicionado que dota al entorno de operaciones de una humedad y temperatura adecuada y constante consiguiendo la protección de los equipos y un óptimo funcionamiento de los mismos.

El equipo de apoyo que suministra energía eléctrica, así como el equipo de aire acondicionado, cuenta con mantenimientos preventivos periódicos a fin de garantizar su correcto funcionamiento.

18.1.4 EXPOSICIÓN AL AGUA

La ER ha tomado las medidas adecuadas para prevenir la exposición al agua de los equipos y el cableado, disponiendo de controles de humedad.

18.1.5 PREVENCIÓN Y PROTECCIÓN CONTRA FUEGO

La ER ha adoptado controles que permiten prevenir y extinguir incendios u otras exposiciones dañinas como llamas o humo en todas sus instalaciones; en tal sentido, los ambientes de la ER, cuentan con detectores de humo, así como extintores que permiten detectar y sofocar un eventual siniestro respectivamente.

18.1.6 ARCHIVO DE MATERIAL

La ER ha establecido lineamientos para la clasificación de la información, así como su tratamiento y condiciones de almacenamiento de acuerdo con la criticidad de esa información y en concordancia con el proceso de certificación digital, las leyes y regulaciones vigentes.

Toda información contenida en formato papel, relacionada con una solicitud de un certificado digital, se almacenará en las instalaciones de la ER, las cuales cuentan con adecuados controles de acceso físico para limitar el acceso solo a personal autorizado, así como proteger dicha información de algún deterioro o daño accidental (ejemplo: agua, incendio, etc.).

Respecto a la información que ingresa en formato electrónico, ésta es almacenada en los equipos (servidores) ubicados en las instalaciones de la ER, en un ambiente que cuenta con controles de acceso físico y lógico para limitar el acceso sólo al personal autorizado. Así también, se protege dicha información de algún daño o destrucción deliberada o accidental (ejemplo: robo, alteración no autorizada, agua, incendio y electromagnetismo). La destrucción de un archivo de auditoría solo se podrá llevar a cabo con la autorización de INDECOPI, siempre y cuando haya transcurrido un periodo mínimo de 10 años

Registro de eventos:

Información de contacto de los solicitantes de los servicios de la ER, incluyendo suscriptores y titulares.
Solicitudes de emisión, re-emisión, revocación, suspensión o modificación de certificados digitales, realizadas mediante un medio no repudiable por parte del titular y/o suscriptor de los certificados.
Resultados y evidencias de cada proceso de validación de identidad de persona jurídica o natural, incluyendo procesos con resultados positivos y procesos fallidos en los que se denegó el servicio a un cliente.
Contratos del suscriptor y titular.
Registros o evidencias de las solicitudes de emisión, re-emisión, revocación, suspensión o modificación de certificados digitales realizadas por parte de los operadores de registro a la Entidad de Certificación, indicando el operador de registro que realizó la transacción.
Registro de contratación de operadores de registro.

Por otro lado, como Entidad Registradora (ER), estamos comprometidos a cumplir con los requisitos relacionados con los recursos necesarios para respaldar nuestras responsabilidades operativas en la Infraestructura de Clave Pública (PKI), manteniendo nuestra solvencia y capacidad para compensar cualquier daño o perjuicio en caso de que estemos obligados a pagar una sentencia o resolución derivada de nuestras operaciones.

Para garantizar esto, hemos establecido disposiciones que incluyen:

Mantenimiento de una cantidad adecuada de cobertura de seguro para cubrir nuestras obligaciones frente a otros participantes.
Acceso a otros recursos para respaldar nuestras operaciones y pagar daños potenciales, que pueden expresarse en términos de un nivel mínimo de activos necesarios para operar y cubrir contingencias dentro de una PKI. Estos recursos pueden incluir activos en nuestro balance general, un bono de garantía, una carta de crédito, o un derecho bajo un acuerdo para una indemnización bajo ciertas circunstancias.
Ofrecimiento de un seguro de responsabilidad civil o garantía de protección a otros participantes en relación con el uso de la PKI.
Además, nos comprometemos a establecer cláusulas de garantía y responsabilidad, incluyendo limitaciones y excepciones, en nuestro Reglamento de Políticas y Seguridad (RPS) o en los contratos con suscriptores o terceros de confianza.

Cuando tercerizamos funciones de registro o custodia de información, garantizamos que tanto nosotros como las organizaciones que realizan estas actividades tercerizadas asumimos la responsabilidad correspondiente. Nos aseguramos de que estas organizaciones actúen de acuerdo con nuestro RPS y otra documentación relevante, estableciendo provisiones de responsabilidad por posibles errores u omisiones.

En el caso de que exista cobertura de seguro o garantías disponibles para suscriptores o terceros de confianza, especificamos los tipos correspondientes en nuestro RPS y en los contratos correspondientes, incluyendo los términos y condiciones de dicha cobertura.

Estas medidas garantizan nuestra solvencia financiera y nuestra capacidad para cumplir con nuestras obligaciones en la PKI, brindando tranquilidad a todos los participantes involucrados

18.1.7 GESTIÓN DE RESIDUOS

La información contenida en formato papel, así como en soportes magnéticos u ópticos, antes de ser eliminada, es destruida tanto física como lógicamente a fin de evitar la posibilidad de recuperación de dicha información desde los formatos que la contuvieren.

Este procedimiento es efectuado de acuerdo con la legislación vigente y las políticas y prácticas de la ER.

18.1.8 COPIA DE SEGURIDAD EXTERNA

Las copias de seguridad de la información correspondiente a la ER, son almacenadas en una plataforma virtual de propiedad de Identity, denominada IDENTITY PKI.

18.2 CONTROLES PROCESALES

18.2.1 ROLES DE CONFIANZA

La ER ha definido y comunicado las funciones a su personal, así mismo se ha determinado los roles de confianza y los procedimientos de control adecuados para el cumplimiento de las obligaciones establecidas en el presente documento. Estos roles son los siguientes:

1. **Gerente de Registro Digital de la ER:**

    1. Es el encargado de aprobar la Política de Seguridad, elaborada en conjunto por el Administrador y Oficial de Seguridad de Información de la ER, y por el Supervisor y Coordinador de Información de la ER.
    2. Es el responsable de coordinar el desarrollo de las auditorías internas a intervalos planificados o cuando ocurran cambios significativos en la puesta en marcha de la seguridad.
    3. Asignará las distintas responsabilidades respecto a la seguridad de la información a las personas involucradas en el proceso de registro o verificación de datos.
    4. Implementará las políticas de seguridad física, las políticas de comunicaciones y redes, las políticas de mantenimiento de equipos y su desecho, las políticas de planificación de contingencias, las políticas de planificación de respuesta a incidentes, las políticas de medios de almacenamiento, y las políticas de manejo de información confidencial, declaradas en la Política de Seguridad.

2. **Administrador y Oficial de Seguridad de Información de la ER:**

    1. Es el encargado de asegurar el cumplimiento de la calidad de servicio de la ER.
    2. Autoriza la emisión de los certificados digitales ante la EC, para lo cual cumplirá y hará cumplir los plazos establecidos para los trámites realizados.
    3. Controla el cumplimiento de las disposiciones legales, reglamento interno, RPS y otras que correspondan a las actividades dentro de la IOFE y; administrará los recursos y bienes que le han sido asignados.

4. Es responsable de la elaboración de la Política de Seguridad, de la supervisión del cumplimiento de la normativa sobre protección de datos personales y la implementación de las acciones respectivas.
5. Supervisará las estrategias, programas, políticas, procedimientos y controles relacionados a la seguridad de la información en el ámbito de la ER.

3. Supervisor y Coordinador de la ER:

1. Es el encargado de velar por el cumplimiento de las funciones de los Operadores de Registro Digital, y distribuir la carga de trabajo entre dichas personas.
2. Autoriza la emisión de los certificados digitales ante la EC BIT4ID, para lo cual cumplirá y hará cumplir los plazos establecidos para los trámites realizados.
3. Controla el cumplimiento de las disposiciones legales, reglamento interno, RPS y otras que correspondan a las actividades dentro de la IOFE.
4. Supervisará el cumplimiento de los procedimientos y directivas de la ER, promoviendo la calidad, eficiencia y eficacia de la operación de la ER.
5. Reportará las fallas e interrupciones de los sistemas y servicios de la ER.
6. Supervisará y apoyará el cumplimiento de las metas de la ER.
7. Es responsable de la elaboración de la Política de Seguridad juntamente con el Administrador y Oficial de Seguridad de Información de la ER.
8. Es responsable de implementar las políticas de planificación de respuesta a incidentes declarada en la Política de Seguridad, juntamente con el Gerente de Registro Digital de la ER.

4. Jefe de Ventas de la ER:

1. Es el encargado de planificar y organizar el trabajo de los Ejecutivos de Ventas y Ejecutivos de Cuentas, conforme a las disposiciones establecidas por la Gerencia General de Identity.
2. Hará cumplir los objetivos, establecidos por la Gerencia General de Identity, para el equipo de ventas, conformado por los ejecutivos descritos en el punto anterior.
3. Tendrá pleno conocimiento de los servicios de registro o verificación de datos de suscriptores y/o titulares, y venta de certificados digitales.

5. Analista de Control Externo:

1. Es el encargado de coordinar con las personas involucradas en el proceso de registro o verificación de datos, a fin de establecer la frecuencia y los recursos necesarios para ejecutar las auditorías internas en el Plan Anual de Auditoria Interna declarado en la Política de Seguridad.

6. Asesor Externo Especialista en Recursos Humanos:

1. Es el responsable de implementar lo estipulado en la Política de Seguridad con respecto a la contratación, renovación, y despido de personal y proveedores vinculados con la ER.

18.2.2 NÚMERO DE PERSONAS REQUERIDAS POR LABOR

La ER mantiene una política rigurosa para asegurarla separación de funciones basado en responsabilidades de trabajo.

La aprobación de la emisión de un certificado digital lo llevarán a cabo mínimo dos personas. Primero el Operador de Registro Digital, quién verificará y/o autenticará la identidad del solicitante,

aprobando o rechazando la solicitud correspondiente, y luego el Supervisor de Registro Digital de la ER quién autorizará la emisión del certificado comunicándolo a la EC, según lo señalado en el procedimiento de trámite de emisión y entrega del certificado digital.

18.2.3 IDENTIFICACIÓN Y AUTENTICACIÓN POR CADA ROL

El personal que opera el sistema administrativo de la ER está autorizado para acceder a la misma previa autenticación de su identidad, doble factor de seguridad, mediante el uso de credenciales digitales como usuario, contraseña y certificado digital personal de autenticación almacenado en un dispositivo criptográfico.

18.3 CONTROLES DE PERSONAL

En esta subsección se establecen los controles implementados por la ER en relación con el personal que desempeña funciones, comprenden entre otros, los requisitos a cumplir para su incorporación, la forma como éstos deben ser comprobados, la capacitación a los que estarán sujetos y las sanciones por acciones no autorizadas. Estos controles alcanzan al personal a cargo de terceros y contratistas que realicen labores por tiempo determinado en las instalaciones de la ER.

18.3.1 CUALIDADES Y REQUISITOS, EXPERIENCIA Y CERTIFICADOS

Los procedimientos y requisitos dispuestos por Identity para la gestión del personal que desarrolla funciones en la ER buscan asegurar que se acredite de manera suficiente y fehaciente las calificaciones y experiencia profesional.

En tal sentido, las prácticas de selección y reclutamiento del personal se llevan a cabo a través de un Asesor Externo especialista en Recursos Humanos, tomando en cuenta los perfiles fijados por la Gerencia General de Identity.

La definición de los puestos de trabajo y sus funciones, se encuentran detalladas en los contratos de trabajo respectivos.

En el caso del personal a cargo de terceros, será responsabilidad del contratista acreditar la formación y experiencia de aquellos, de acuerdo con los requerimientos fijados por la Gerencia General de Identity, debiendo presentar la documentación que evidencie el cumplimiento de dicho aspecto.
El personal de la ER deberá firmar términos contractuales respecto de la protección de la privacidad y confidencialidad de toda la información presentada por los clientes de la ER. Los responsables de administrar los sistemas para solicitar la emisión, re-emisión, revocación, suspensión o modificación de los certificados digitales deben contar con experiencia y conocimiento en el uso de certificados digitales o seguridad de la información

18.3.2 PROCEDIMIENTO PARA VERIFICACIÓN DE ANTECEDENTES

Es política de Identity verificar la documentación aportada por el personal aspirante a realizar labores en la ER. Para tal efecto, el Asesor Externo especialista en Recursos Humanos, ejecuta los siguientes controles mínimos:

- ✓ Verificación de la identidad personal.
- ✓ Confirmación de las referencias.
- ✓ Confirmación de empleos anteriores.
- ✓ Revisión de referencias profesionales.
- ✓ Confirmación de grados académicos obtenidos.
- ✓ Verificación de antecedentes penales, policiales, crediticios, entre otros

En caso de personal a cargo de terceros, corresponde al contratista realizar la verificación de los antecedentes respectivos de sus empleados.

18.3.3 REQUISITOS DE CAPACITACIÓN

Es política de Identity que toda persona que desarrolla funciones en la ER, reciba desde su ingreso una instrucción- inducción acorde con la función a desempeñar. Dicho personal se encontrará sujeto a un plan de capacitación continuo, a fin que las responsabilidades asumidas como parte de los servicios de certificación digital se desarrollen en forma competente.

El contenido de los programas de capacitación se controla y refuerza periódicamente por la Gerencia de Registro Digital, en coordinación con el Administrador de la ER, llevándose un registro y archivo de las materias impartidas para los efectos de las re-capacitaciones.

El plan de capacitación, adecuado a las funciones a desempeñar en la ER, contiene como mínimo los siguientes conceptos básicos:

- ✓ Uso y operación del hardware y software empleado.
- ✓ Aspectos relevantes de la "Declaración de Prácticas y Políticas de Registro", "Política de Seguridad", "Política de Privacidad", "Plan de Privacidad", y otra documentación que comprenda sus funciones.
- ✓ Marco regulatorio de la prestación de los servicios de certificación digital.
- ✓ Procedimientos en caso de contingencias.
- ✓ Procedimientos de operación, administración y seguridad para cada rol específico.

La Gerencia de Registro Digital de la ER, juntamente con la Administración de la ER, cuando estimen conveniente o por disposición legal expresa, podrá incluir otros temas en la capacitación con la finalidad de lograr una apropiada formación y alcanzar un adecuado proceso de mejora continua de la capacitación del personal.

18.3.4 FRECUENCIA Y REQUISITOS DE LAS RE-CAPACITACIONES

La re-capacitación se efectuará necesariamente cuando el personal sea sustituido o rotado, así como cuando se realicen cambios en los procedimientos de operaciones o en la "Declaración de Prácticas y Políticas de Registro", "Política de Seguridad", "Política de Privacidad", y "Plan de Privacidad", o en cualquier otro documento que resulte relevante para la ER y que comprometa los aspectos funcionales de las labores del personal.
El personal de la ER, que administra los sistemas para la solicitud, re-emisión, revocación, modificación o suspensión, debe recibir una capacitación continua respecto:

- Certificados digitales
- Firma digital
- Regulación de la IOFE
- Política de registro.
- Políticas de seguridad y privacidad de la ER
- RPS
- Plan de contingencia
- Funciones respecto de su rol.
- Seguridad de la Información.

La frecuencia de la capacitación deberá ser de al menos una vez antes de operar en la ER y luego de manera anual.

18.3.5 FRECUENCIA Y SECUENCIA DE LA ROTACIÓN EN EL TRABAJO

La ER, en caso determine la conveniencia, podrá implementar rotaciones de trabajo entre los distintos roles, con el objeto de incrementar la seguridad y asegurar la continuidad de las actividades. La rotación es comunicada al personal con el documento pertinente.

18.3.6 SANCIONES POR ACCIONES NO AUTORIZADAS

Le es aplicable a todo el personal el Reglamento Interno de Identity, independientemente de la modalidad de contratación.

Con relación a las operaciones de la ER, se considerarán acciones no autorizadas, aquellas realizadas por el personal de manera negligente o malintencionada y que contravengan la presente "Declaración de Prácticas y Políticas de Registro", "Política de Seguridad", "Política de Privacidad", y "Plan de Privacidad", así como las directivas, guías de procedimientos, reglamento interno, y demás documentos afines.

La ER apenas tome conocimiento de la acción no autorizada o de su potencial ejecución, suspenderá el acceso a todos los sistemas de información a aquel personal que se encuentre involucrado en el hecho.

Con la confirmación del hecho, el Administrador de la ER, informará a la Gerencia General de Identity, a fin de que ésta autorice al Área Legal para que inicie el procedimiento sancionador correspondiente, y de ser el caso se inicien las acciones legales para el resarcimiento por los daños y perjuicios en lo que pudiera verse afectado.

18.3.7 DOCUMENTACIÓN SUMINISTRADA AL PERSONAL DE IDENTITY

La ER suministra a todo su personal, en función a los cargos y roles que desempeñe, la documentación mínima siguiente:

- ✓ Manual de funcionamiento de equipos y software que debe operar en la ER.
- ✓ "Declaración de Prácticas y Políticas de Registro", "Política de Seguridad", "Política de Privacidad", y "Plan de Privacidad".
- ✓ Normas legales y marco regulatorio aplicables a sus funciones en la ER.
- ✓ Documentación aplicable en caso de contingencias.
- ✓ Otra documentación relevante con relación a sus funciones en la ER.

A fin de verificar que el personal tenga conocimiento de sus roles, se debe obtener una constancia por escrito de dichas capacitacioes

18.4 GESTIÓN DE OPERACIONES

18.4.1 MÓDULO CRIPTOGRÁFICO

La generación de claves de los suscriptores debe ser realizada en módulos criptográficos FIPS 140-2.

Los módulos criptográficos usados por los Operadores de Registro deben cumplir los requerimientos o ser equivalentes a los requerimientos de FIPS 140-2 nivel de seguridad 2 como mínimo.
Se les hace entrega de sus claves mediante su correo electrónico, verificando previamente que sea del titular, de esta manera garantizamos la entrega.

18.4.2 RESTRICCIONES DE LA GENERACIÓN DE CLAVES

Las claves pueden ser generadas solamente por los propios suscriptores.

18.4.3 ENTREGA DE LA CLAVE PÚBLICA

Cuando un suscriptor genera su propio par de claves o par de claves del titular, las claves públicas correspondientes deben ser entregadas al emisor del certificado de manera tal que se asegure la autenticidad de dicho suscriptor.

En los casos en que las ERs acepten las claves públicas en representación de los emisores de los certificados, éstas deberán ser entregadas a dicho emisor de manera tal que se asegure el mantenimiento de la asociación que debe existir entre el titular y la clave.

18.4.4 DEPÓSITO DE LA CLAVE PÚBLICA

La ER no genera copias de las claves privadas de los suscriptores ni de los Operadores de Registro en ninguna modalidad.

18.4.5 DATOS DE ACTIVACIÓN

Los datos de activación del módulo criptográfico serán administrados por los suscriptores. En caso de obtener módulos criptográficos de Identity se brindará la información correspondiente para realizar la asignación de los de activación por canales seguros.

19. AUDITORÍAS

19.1 FRECUENCIA DE AUDITORÍAS

La ER, efectuará auditorías internas al menos una vez al año.

Las evaluaciones técnicas del INDECOPI se llevarán cada vez que la Autoridad Administrativa Competente lo requiera.
Los registros deben ser revisados como parte de la auditoría de la AAC, de manera anual

19.2 CALIFICACIONES DE LOS AUDITORES

La selección de los auditores depende del INDECOPI.

- Auditorias de registros: los registros deben ser revisados como parte de la auditoria de la AAC, de manera anual.
- Auditorias del archivo: el archivo debe ser revisado como parte de la auditoria de la AAC, de manera anual
- Auditoria de los procedimientos y controles: los procedimientos y controles implementados deben ser auditados por la AAC de manera anual. Las auditorias internas deben llevarse a cabo, como mínimo, una vez al año en la ER

19.3 RELACIÓN DEL AUDITOR CON LA ER

Los auditores o asesores deben ser independientes de la ER.
Los sistemas de registro deben generar registros de auditoría sobre las solicitudes de emisión, re-emisión, revocación, modificación o suspensión de certificados, indicando el personal que hizo la solicitud y el resultado positivo o fallido de la misma.

20. MATERIAS DE NEGOCIO Y LEGALES

20.1 TARIFAS

Las tarifas por los servicios de registro y certificación digital serán proporcionadas a los clientes, a través de los Ejecutivos de Ventas de la ER. Directamente, mediante correo electrónico.

20.2 POLÍTICAS DE REEMBOLSO

Las políticas de reembolso por los servicios de registro serán definidas en "El Contrato".

20.3 COBERTURA DE SEGURO

Identity proporciona a sus clientes servicios de registro amparados por la cobertura del Seguro de Responsabilidad Civil de la Entidad de Certificación AC BIT4ID.

20.4 PROVISIONES Y GARANTÍAS

Las garantías por los servicios de registro y certificación digital serán definidas en "El Contrato", 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.

20.5 EXCEPCIONES DE GARANTÍAS

La ER 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.

20.6 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.

20.7 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.
El incumplimiento de las responsabilidades relacionadas con la clave privada puede acarrear serias consecuencias legales. En primer lugar, la exposición, el riesgo o el uso indebido de la clave privada pueden comprometer la seguridad de la información protegida, lo que puede resultar en daños significativos para todas las partes involucradas. Además, cualquier deterioro, alteración o manipulación de la clave privada podría invalidar su autenticidad y poner en duda la integridad de los documentos o transacciones firmadas digitalmente.

Otro aspecto crucial es la revocación de las facultades de representación y/o poderes de los representantes legales o apoderados asociados con la clave privada. Esta revocación puede tener repercusiones legales graves en términos de autoridad y capacidad para actuar en nombre de una entidad.

Asimismo, si la información contenida en el certificado ya no es precisa o el suscriptor deja de cumplir con los requisitos de membresía en la comunidad de interés pertinente, el certificado podría volverse inválido, lo que podría afectar la validez de las transacciones realizadas con él.

Por último, el incumplimiento de las obligaciones estipuladas en el contrato del suscriptor y/o titular dentro de la Infraestructura de Clave Pública (IOFE) puede acarrear sanciones legales y la posible terminación de los servicios proporcionados.

En resumen, la responsabilidad en el manejo y protección de la clave privada es fundamental para garantizar la seguridad y la validez de las transacciones electrónicas, y su incumplimiento puede tener serias implicaciones legales.

Los potenciales terceros que confían deben conocer sus obligaciones para validar un certificado al momento de la transacción, así como las consecuencias de omisiones. Las EC notifican a los terceros que confían sobre la revocación de un certificado, a menudo mediante la publicación de un documento accesible para todos los terceros involucrados, advirtiendo sobre la forma de dicha publicación y sus implicaciones

Debe indicarse claramente que la función de registro no se terciariza y, por lo tanto, no aplica. En caso de tercerizar las funciones de registro, las responsabilidades de los terceros deberán ser claramente definidas en la RPS. Sin embargo, la responsabilidad legal frente a la IOFE, los suscriptores, titulares y terceros que confían es de la entidad solicitante de la acreditación de la Entidad de Registro.

La Entidad de Registro tiene la obligación de garantizar la seguridad y protección de los datos personales y confidenciales de la ER, así como la integridad y autenticidad de las transacciones en la autorización de solicitudes de emisión, revocación, reemisión, durante la ejecución de las actividades de tercerización

20.8 INDEMNIZACIÓN

Los casos de indemnización están establecidos en “El Contrato”.

20.9 NOTIFICACIONES

Los medios de notificación están establecidos en “El Contrato”.

20.10 ENMENDADURAS Y CAMBIOS

Las enmendaduras y cambios serán comunicadas al INDECOPI y luego de su aprobación serán publicadas en el repositorio y notificadas a los titulares y suscriptores, conforme a los medios especificados en sus contratos.

20.11 RESOLUCIÓN DE DISPUTAS

El procedimiento de resolución de disputas está establecido en “El Contrato”.

20.12 CONFORMIDAD CON LA LEY APLICABLE

La ER se compromete a cumplir la Ley aplicable a las operaciones de registro: las Guías de Acreditación de Entidades de Registro o Verificación del INDECOPI, la Ley de Firmas y Certificados Digitales y su Reglamento.

20.13 SUBROGACIÓN

La ER no delega sus responsabilidades respecto de las operaciones de registro sobre terceros no autorizados por la IOFE. Todos los casos de responsabilidad de otros participantes como las EC son especificados en este documento.

20.14 FUERZA MAYOR

Las cláusulas de fuerza mayor están establecidas en “El Contrato”.

20.15 DERECHOS DE PROPIEDAD INTELECTUAL

Todos los derechos de propiedad intelectual incluyendo los que corresponden a las aplicaciones o software desarrollado para las actividades de la ER, OIDs, la presente “Declaración de Prácticas y Políticas de Registro”, “Política de Seguridad”, “Política de Privacidad”, y “Plan de Privacidad”, así como cualquier otro documento, electrónico o de cualquier otro tipo, son propiedad de Identity. Por tanto, se prohíbe cualquier acto de reproducción, distribución, comunicación pública y transformación de cualquiera de los elementos que son de titularidad de Identity.

Las claves privadas y las claves públicas son propiedad del titular del certificado digital.

21. FINALIZACIÓN DE LA ER

Antes de su finalización, la ER informará al INDECOPI, a los suscriptores, titulares y terceros que confían sobre el cese de sus operaciones con por lo menos treinta (30) días calendario de anticipación.

Todas las solicitudes y contratos de suscriptores y titulares serán transferidos al INDECOPI o a otro PSC designado por éste.

En caso de una operación de transferencia de titularidad, los nuevos dueños u operadores solicitarán la evaluación de cumplimiento al INDECOPI para garantizar que se mantienen los requisitos de acreditación.

Se advertirá a todos los suscriptores, titulares y terceros que confían, respecto a los cambios y todo tipo de condición asociada a la continuidad del uso de los certificados emitidos por una EC que finaliza o transfiere sus operaciones, mediante un comunicado publicado en la siguiente dirección:
La comunicación a la AAC será con 60 dias de anticipación
Por otro lado, la ER brinda las siguientes medidas por si acordamos finalizar

- Establecer un proceso automatizado para la transferencia regular de los registros de auditoría a la AAC o entidad designada, asegurando su integridad y confidencialidad durante el tránsito.
- Implementar un sistema de almacenamiento seguro y protegido para los registros de auditoría, con acceso restringido y controlado únicamente por personal autorizado.
- Realizar copias de seguridad periódicas de los registros de auditoría y almacenarlas en ubicaciones geográficamente dispersas para mitigar riesgos de pérdida de datos.
- Establecer protocolos claros y detallados para la finalización de actividades, que incluyan la revisión y cumplimiento de todas las cláusulas de garantías y responsabilidades establecidas.
- Designar a un responsable de cumplimiento que supervise el proceso de transferencia de registros y garantice que se cumplan todos los requisitos y plazos establecidos por la AAC.
- Capacitar al personal sobre los procedimientos y responsabilidades relacionadas con la transferencia de registros y el cumplimiento de garantías, asegurando un entendimiento claro de los procesos involucrados.
- Realizar auditorías internas periódicas para verificar el cumplimiento de los procedimientos establecidos y tomar medidas correctivas si se identifican áreas de mejora.
- Mantener una comunicación fluida y transparente con la AAC o entidad designada, informando sobre cualquier cambio en los procedimientos o dificultades que puedan surgir durante la transferencia de registros.

Estas medidas contribuirán a garantizar que los registros de auditoría se transfieran de manera segura y oportuna, cumpliendo con las obligaciones contractuales y regulatorias, y preservando la integridad y confidencialidad de la información.

22. BIBLIOGRAFIA

En la redacción de la presente RPS, se utilizó:

- Ley N° 27269, Ley de Firmas y Certificados Digitales.
- Reglamento de la Ley de Firmas y Certificados Digitales aprobado mediante el Decreto Supremo N° 052-2008-PCM, y sus modificatorias, el Decreto Supremo N° 070-2011-PCM, y Decreto Supremo N° 105-2012-PCM.
- Ley N° 29733, Ley de Protección de Datos Personales.
- Guía de Acreditación de Entidad de Registro, Versión 3.3 - INDECOPI.
- Norma Marco sobre Privacidad para los países integrantes del APEC, aprobada en la 16° Reunión Ministerial del APEC, Santiago de Chile, 17 y 18 de noviembre de 2004.