BIGDAVI

INNOVACIÓN Y CONFIANZA

CÓDIGO: POL-ACR-002

POLITICA DE REGISTRO

SISTEMA INTEGRADO DE GESTIÓN (SIG) / Versión:2.0 / Fecha: Octubre 2026

APROBADO POR:	**Nombre:** Wilfredo Dávila **Cargo:** Gerente General **Fecha:** 15/10/2026	**Firma:** BIGDAVI Firma Digital Firmado digitalmente por: WILFREDO ALBERTICO DAVILA FUENTES Área: GERENCIA GENERAL Cargo: GERENTE GENERAL Empresa: BIGDAVI S.A.C. Motivo: Actualizacin v.2.0 Localidad: Lima Fecha: 2026.10.16 11:19:56 -0500
REVISADO POR:	**Nombre:** Jesús Ojeda **Cargo:** Gerente de Operaciones **Fecha:** 15/10/2026	**Firma:** BIGDAVI Firma Digital Firmado digitalmente por: JESUS MANUEL OJEDA ANGLES Cargo: Gerente de Operaciones Empresa: BIGDAVI S.A.C. Motivo: Actualización v.2.0 Localidad: Lima Fecha: 2026.10.16 08:50:04 -0500
ELABORADO POR:	**Nombre:** Grecia Canales **Cargo:** Coordinadora SIG **Fecha:** 15/10/2026	**Firma:** BIGDAVI Firma Digital Firmado digitalmente por: GRECIA ANAHI CANALES RIOS Cargo: Coordinadora SIG Empresa: BIGDAVI S.A.C. Motivo: Actualización v.2.0 Localidad: Lima Fecha: 2026.10.15 18:01:04 -0500

INDICE

1. Introducción 7
2. Objetivo 7
3. Participantes 7
4. Definiciones y abreviaciones 8
5. Uso apropiado del certificado 9
6. Administración de políticas 9
6.1. Organización que administra los documentos de rps 9
6.2. Procedimiento de aprobación de rps 9
7. Publicación y registro 9
7.1. Publicación de la información sobre certificación 9
7.2. Tiempo o frecuencia de la publicación 9
7.3. Controles de acceso a los registros 10
8. Identificación y autenticación 10
8.1. Reconocimiento, autenticación y rol de las marcas registradas 10
8.2. Validación inicial de la identidad 11
8.2.1. Método para probar la poseción de la clave privada 11
8.2.2. Autenticación de la identidad de una persona jurídica 11
8.2.3. Autenticación de la identidad de persona natural 12
8.2.4. Información no verificada del suscriptor 12
8.2.5. Validación de la autoridad 12
8.3. Identificación y autenticación para solicitudes de re-emisión de certificado 12
8.3.1. Identificación y Autenticación para solicitudes de remisión de certificad os rutinaria 13
8.3.2. Identificación y Autenticación para la re-emisión de certificado luego de la revocación 13
8.4. Identificación y autenticación para la solicitud de revocación 13
9. Requisitos operacionales del ciclo de vida de los certificados 14
9.1. Solicitud del certificado 14
9.1.1. Habilitados para presentar la solicitud de un certificado 14

Documento de uso interno. Su contenido es confidencial y está destinado exclusivamente al personal autorizado de BIGDAVI S.A.C. Queda prohibida su reproducción, distribución o divulgación sin la autorización expresa de la Gerencia.

9.1.2. Proceso de solicitud y responsabilidades 14
9.2. Procesamiento de la solicitud de un certificado 14
9.2.1. Realización de las funciones de identificación y autenticación 14
9.2.2. Aprobación o rechazo de la solicitud de certificado 15
9.2.3. Tiempo para el procesamiento de la solicitud de un certificado 16
9.3. Re-emisión de certificado 16
9.3.1. Circunstancias para la re-emisión de un certificado 16
9.3.2. Personas habilitadas para solicitar la reemisión de certificado 16
9.3.3. Procesamiento de las solicitudes para re-emisión de certificados 17
9.4. Revocación y suspensión del certificado 17
9.4.1. Circunstancias para la revocación 17
9.4.2. Personas habilitadas para solicitar la revocación 18
9.4.3. Procedimiento para la solicitud de revocación 18
9.4.4. Circunstancias para la suspensión 18
9.4.5. Personas habilitadas para solicitar la suspensión 19
9.4.6. Procedimiento para la solicitud de la suspensión 19
9.4.7. Límite del periodo de suspensión 19
10. Controles de las instalaciones, de la gestion y controles operacionales 19
10.1. Controles físicos 19
10.1.1. Ubicación y construcción del local 19
10.1.2. Acceso físico 19
10.1.3. Energía y aire acondicionado 20
10.1.4. Exposición al agua 20
10.1.5. Prevención y protección contra fuego 20
10.1.6. Archivo de material 20
10.1.7. Gestión de residuos 20
10.1.8. Copia de seguridad externa 20
10.2. Controles procesales 20
10.2.1. Roles de confianza 20
10.2.2. Número de personas requeridas por labor 21
10.2.3. Identificación y autenticación para cada rol 21
10.2.4. Roles que requieren funciones por separado 21

Documento de uso interno. Su contenido es confidencial y está destinado exclusivamente al personal autorizado de BIGDAVI S.A.C. Queda prohibida su reproducción, distribución o divulgación sin la autorización expresa de la Gerencia.

10.3. Controles de personal 21
10.3.1. Cualidades y requisitos, experiencia y certificados 21
10.3.2. Procedimiento para verificación de antecedentes 21
10.3.3. Requisitos de capacitación 22
10.3.4. Frecuencia y requisitos de las re•capacitaciones 22
10.3.5. Frecuencia y secuencia de la rotación en el trabajo 22
10.3.6. Sanciones por acciones no autorizadas 22
10.3.7. Requerimientos de los contratistas 22
10.3.8. Documentación suministrada al personal 22
10.4. Procedimiento de registro de auditorías 23
10.4.1. Tipos de eventos registrados 23
10.4.2. Frecuencia del procesamiento del registro 23
10.4.3. Periodo de conservación del registro de auditorías 23
10.4.4. Protección del registro de auditoría 23
10.4.5. Procedimiento de copia de seguridad del registro de auditorías 23
10.4.6. Sistema de realización de auditoría (Interna vs Externa) 24
10.4.7. Notificación al titular que causa un evento 24
10.4.8. Valoración de vulnerabilidad 24
10.5. Archivo de registro 24
10.5.1. Tipos de eventos registrados 24
10.5.2. Periodo de conservación del archivo 24
10.5.3. Protección del archivo 24
10.5.4. Procedimientos para copia de seguridad del archivo 24
10.5.5. Requisitos para los archivos de sellado de tiempo 25
10.5.6. Sistema de recolección del archivo (Interna o Externa) 25
10.5.7. Procedimiento para obtener y verificar la información del archivo 25
10.6. Recuperación frente al compromiso y desastre 25
10.6.1. Procedimiento de manejo de incidentes y compromisos 25
10.6.2. Adulteración de los recursos computacionales, software y/o datos 25
10.7. Finalización de la EC o ER 26
11. Controles de seguridad técnica 26
11.1. Generación e instalación del par de claves 26

Documento de uso interno. Su contenido es confidencial y está destinado exclusivamente al personal autorizado de BIGDAVI S.A.C. Queda prohibida su reproducción, distribución o divulgación sin la autorización expresa de la Gerencia.

11.1.1. Generación del par de claves 26
11.1.2. Entrega al suscriptor de la clave privada 26
11.1.3. Entrega de la clave pública para el emisor de un certificado 26
11.2. Controles de ingeniería para protección de la clave privada y módulo criptográfico 27
11.2.1. Estándares y controles para el módulo criptográfico 27
11.2.2. Depósito de clave privada 27
11.2.3. Archivo de la clave privada 27
11.2.4. Clasificación del módulo criptográfico 27
11.3. Datos de activación 27
11.3.1. Otros aspectos de los datos de activación 27
11.4. Controles de seguridad computacional 28
11.4.1. Requisitos técnicos específicos para seguridad computacional 28
11.4.2. Evaluación de la seguridad computacional 28
12. Auditorias de compatibilidad y otras evaluaciones 28
12.1. Frecuencia y circunstancias de la evaluación 28
12.2. Identidad/Calificaciones de asesores 28
12.3. Relación del auditor con la entidad auditada 28
12.4. Elementos cubiertos por la evaluación 28
12.5. Acciones a ser tomadas frente a resultados deficientes 29
13. Otras materias de negocio y legales 29
13.1. TARIFAS 29
13.1.1. Tarifas para la emisión o renovación de certificados 29
13.1.2. Tarifas para otros servicios 29
13.1.3. Políticas de reembolso 29
13.2. Responsabilidad financiera 29
13.2.1. Cobertura de seguro 29
13.2.2. Cobertura de seguro o garantía para entidades finales 30
13.3. Confidencialidad de la información del negocio 30
13.3.1. Alcances de la información confidencial 30
13.3.2. Información no contenida dentro del rubro de información confidencial 30
13.3.3. Responsabilidad de protección de la información confidencial 30
13.4. Privacidad de la información personal 30

Documento de uso interno. Su contenido es confidencial y está destinado exclusivamente al personal autorizado de BIGDAVI S.A.C. Queda prohibida su reproducción, distribución o divulgación sin la autorización expresa de la Gerencia.

13.4.1. Plan de privacidad 30
13.4.2. Información tratada como privada 31
13.4.3. Información no considerada privada 31
13.4.4. Notificación y consentimiento para el uso de información 31
13.4.5. Divulgación realizada con motivo de un proceso judicial o administrativo 31
13.4.6. Otras circunstancias para divulgación de información 32
13.5. Derecho de propiedad intelectual 32
13.6. Representaciones y garantías 32
13.6.1. Representaciones y garantías de la ER 32
13.6.2. Representaciones y garantías de los suscriptores 32
13.6.3. Representaciones y garantías de las terceros que confían 32
13.6.4. Representaciones y garantías de otros participantes 33
13.7. Exención de garantías 33
13.8. Indemnizaciones 33
13.9. Término y terminación 33
13.9.1. Término 33
13.9.2. Terminación 33
13.9.3. Efecto de terminación y supervivencia 34
13.11. Enmendaduras 34
13.11.1. Procedimiento para enmendaduras 34
13.11.2. Mecanismos y periodo de notificación 34
13.12. Provisiones sobre resolución de disputas 34
13.13. Ley aplicable 34
13.14. Conformidad con la ley aplicable 34
13.15. Cláusulas misceláneas 35
13.15.1. Acuerdo íntegro 35
13.15.2. Subrogación 35
13.15.3. Ejecución (tarifas de abogados y cláusulas de derechos) 35
13.15.4. Fuerza mayor 35
13.15.5. Otras cláusulas 35
14. Control de cambios 35

Documento de uso interno. Su contenido es confidencial y está destinado exclusivamente al personal autorizado de BIGDAVI S.A.C. Queda prohibida su reproducción, distribución o divulgación sin la autorización expresa de la Gerencia.

1. Introducción

BIGDAVI S.A.C., se constituye como Entidad de Registro o Verificación de la Entidad de Certificación CAMERFIRMA PERÚ S.A.C., y brinda servicios de recepción de solicitudes de emisión, de revocación, re-emisión y suspensión de los certificados digitales, tanto para el caso de personas jurídicas como personas naturales respecto de los servicios brindados por esta Entidad de Certificación.

2. Objetivo

BIGDAVI S.A.C., como Entidad de Registro o Verificación, tiene como objetivo asegurar la confiabilidad de la identidad del solicitante de los servicios de emisión, revocación, re-emisión y suspensión de los certificados digitales, registrando y verificando la información entregada por los solicitantes antes de comunicar a la Entidad de Certificación la aprobación de una solicitud. Y dar cumplimiento a las normas, polÍticas y directrices establecidos por CAMERFIRMA PERÚ S.A.C. para sus Entidades de Registro a nivel internacional.

3. Participantes

- CAMERFIRMA PERÚ S.A.C.: Entidad emisora de certificados digitales, las cual utilizan los servicios de registro de BIGDAVI S.A.C. La información respecto a la Entidad de Certificación CAMERFIRMA PERÚ S.A.C., así como sus Políticas de Certificación, sus Declaraciones de Prácticas y respectivos convenios se encuentran publicados en la siguiente dirección web: http://www.camerfirma.com.pe

  CAMERFIRMA PERÚ S.A.C., brinda el servicio web de registro, mediante el cual BIGDAVI S.A.C., gestionará la aprobación de las solicitudes de los servicios de certificación digital, por lo que la responsabilidad de la disponibilidad y seguridad de estos sistemas depende de CAMERFIRMA PERÚ S.A.C.

  CAMERFIRMA PERÚ S.A.C., cuenta con la Certificación de WebTrust y vela por el reconocimiento legal de la Autoridad Administrativa competente, INDECOPI.

- BIGDAVI S.A.C.: Entidades de Registro o Verificación: BIGDAVI S.A.C., reside en el Perú y se somete ante el proceso de acreditación del INDECOPI. Las comunicaciones entre la ER y CAMERFIRMA PERÚ S.A.C.., se realizan vía web de manera ininterrumpida, según los niveles de disponibilidad y recuperación brindados y declarados por cada EC. La ER tiene procedimientos de contingencia para acceder a los sistemas en casos de corte del servicio de Internet. La disponibilidad del servicio web de registro es provista por cada EC y es responsabilidad de CAMERFIRMA PERÚ S.A.C.., el mecanismo de contingencia utilizado.

- Titulares de certificados: La comunidad de usuarios definidos como titulares de los certificados digitales será definida según lo establecido en la Política de Certificación y Declaración de Prácticas de cada Entidad de Certificación a la que la ER de BIGDAVI S.A.C., se encuentra vinculada.

  La ER de BIGDAVI S.A.C., brinda servicios solamente a personas naturales o jurídicas. En el caso de personas naturales, los servicios de validación serán brindados a personas sin impedimento legal de nacionalidad peruana.

Documento de uso interno. Su contenido es confidencial y está destinado exclusivamente al personal autorizado de BIGDAVI S.A.C. Queda prohibida su reproducción, distribución o divulgación sin la autorización expresa de la Gerencia.

- Terceros que confían: Los terceros que confían son personas naturales o jurídicas que confían en el contenido y la aplicación de un certificado digital. En este sentido, los terceros que confían pueden ser todas aquellas personas naturales y jurídicas que requieren evaluar la validez de un certificado para proceder con sus respectivas transacciones electrónicas, incluyendo entidades de otras infraestructuras además de la IOFE.

  La comunidad de usuarios definidos como terceros que confían, dependerá de lo establecido en la Política de Certificación y Declaración de Prácticas de cada Entidad de Certificación a la que la ER de BIGDAVI S.A.C., se encuentra vinculada.

4. Definiciones y abreviaciones

Término	Definición
Entidad de Certificación (EC)	Es la persona jurídica pública 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)	Es la persona jurídica, con excepción de los notarios públicos, encargada del levantamiento de datos, la comprobación de éstos respecto a un solicitante de un certificado digital, la aceptación y autorización de las solicitudes para la emisión de un certificado digital, así como de la aceptación y autorización de las solicitudes de cancelación de certificados digitales. Las personas encargadas de ejercer la citada función serán supervisadas y reguladas por la normatividad vigente.
Declaración de Prácticas de Registro (RPS)	Conjunto de declaraciones sobre políticas y prácticas de la Entidad de Registro, que sirve para comunicar el cumplimiento legal y regulatorio a los suscriptores y terceros que confían.
Operador de Registro	Persona responsable de representar a BIGDAVI S.A.C., en calidad de ER de CAMERFIRMA PERÚ S.A.C., en las actividades de recepción, validación y procesamiento de solicitudes.
Prácticas de Registro	Son las prácticas que establecen las actividades y requerimientos de seguridad y privacidad correspondientes al Sistema de Registro o Verificación de una Entidad de Registro o Verificación.
Prestadores de servicios de certificación digital (PSC)	El conjunto de participantes de la IOFE, ER, EC, SVA y proveedores de aplicaciones de software.
Suscriptor	Es la 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 digital sea una persona natural, sobre ella recaerá la responsabilidad de suscriptor. En el caso que una persona jurídica sea el titular de un certificado digital, la responsabilidad de suscriptor recaerá sobre el representante legal designado por esta entidad. Si el certificado

Documento de uso interno. Su contenido es confidencial y está destinado exclusivamente al personal autorizado de BIGDAVI S.A.C. Queda prohibida su reproducción, distribución o divulgación sin la autorización expresa de la Gerencia.

	está designado para ser usado por un agente automatizado, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderán a la persona jurídica. La atribución de responsabilidad de suscriptor, para tales efectos, corresponde a la misma persona jurídica.
Titular	Es la persona natural o jurídica a quien se le atribuye de manera exclusiva un certificado digital.
Tercero que confía	Se refiere a las 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.

5. Uso apropiado del certificado

Los criterios para definir el uso apropiado, rango de acción o aplicabilidad de un certificado digital solicitado a BIGDAVI S.A.C. en calidad de ER dependerá de lo establecido en la Política de Certificación y Declaración de Prácticas de cada AC para las que BIGDAVI S.A.C. brinda el servicio de ER.

6. Administración de políticas

6.1. Organización que administra los documentos de rps

Los detalles de contacto se encuentran registradas en la RPS de BIGDAVI S.A.C., tal como lo indica la AAC.

6.2. Procedimiento de aprobación de rps

INDECOPI, en su calidad de Autoridad Administrativa Competente (AAC), aprueba la RPS de las ERs luego de ejecutados los procedimientos establecidos en la Guía de Acreditación de Entidades de Registro y comprobada su correcta observancia.
https://bigdavi.com/certificaciones-y-acreditaciones/#

7. Publicación y registro

7.1. Publicación de la información sobre certificación

La Declaración de Prácticas de Registro y toda la documentación pertinente y relevante vigente de BIGDAVI S.A.C. en calidad de ER, así como sus versiones
anteriores, son publicadas en la siguiente dirección web:

7.2. Tiempo o frecuencia de la publicación

Las modificaciones relativas a la RPS u otra documentación de la ER de BIGDAVI S.A.C., deben ser publicadas tan pronto como razonablemente sea posible, debiendo tener cuidado de cumplir con los requisitos que fueren necesarios para la aprobación de dichas modificaciones.
Toda modificación relativa a la RPS debe ser aprobada por INDECOPI antes de su publicación.

Documento de uso interno. Su contenido es confidencial y está destinado exclusivamente al personal autorizado de BIGDAVI S.A.C. Queda prohibida su reproducción, distribución o divulgación sin la autorización expresa de la Gerencia.

7.3. Controles de acceso a los registros

El acceso a los registros debe ser restringido únicamente para el uso de los titulares y suscriptores legítimos, así como a los trabajadores competentes dentro de la ER, teniendo en cuenta los temas de privacidad que pudieran existir en los contratos de los suscriptores o titulares y en conformidad con la Norma Marco sobre Privacidad.
La ER debe emplear sistemas fiables para el registro, de modo tal que:

- Únicamente personas autorizadas tengan acceso a lectura y modificaciones.
- Pueda comprobarse la autenticidad de la información.

8. Identificación y autenticación

BIGDAVI S.A.C. en su RPS describe los procedimientos y criterios utilizados para autenticar la identidad y/o otros atributos de un solicitante de certificado, mediante la verificación presencial de la identidad del solicitante. Además se describen los procedimientos para autenticar las partes que solicitan revocación, re-emisión o suspensión de certificados (la habilitación de los últimos tres procesos mencionados dependerá de lo establecido por cada EC en su respectiva CPS para la cual se brinde el servicio de ER). En el caso del proceso de solicitud de revocación de un certificado, se requerirá la presencia física del solicitante para todos los casos en los que dicho solicitante es una persona distinta al suscriptor del certificado (titulares, terceros o representantes legalmente autorizados). Los suscriptores podrán también presentarse en la ER para realizar sus solicitudes, pero dicha acción no será obligatoria a menos que la EC no establezca en su CPS otros mecanismos de solicitud (por ejemplo, a través de mecanismos telemáticos).

En los casos que los certificados sean emitidos para ser usados por agentes automatizados, el proceso de validación para la vinculación entre el certificado y el agente será también claramente establecido en la RPS.
La EC correspondiente debe establecer el procedimiento para la prueba de posesión de la clave privada y su almacenamiento en módulos acreditados según el Common Criteria, FIPS140-2 o equivalente, con la declaración del número de serie del módulo, factura o auditoría respectiva, por ejemplo.

8.1. Reconocimiento, autenticación y rol de las marcas registradas

Se prohíbe a los solicitantes de certificados de personas jurídicas que incluyan nombres en las solicitudes que puedan suponer infracción de derechos de terceros.
En el caso de personas jurídicas, no se podrá volver a asignar un nombre de titular que ya haya sido asignado a un titular diferente.
No le corresponde a la ER determinar si un solicitante de certificados le asiste algún tipo de derecho sobre el nombre que aparece en una solicitud de certificado. Asimismo, no le corresponde resolver ninguna disputa concerniente a la propiedad de nombres de personas naturales o jurídicas, nombres de dominio, marcas o nombres comerciales. Sin embargo, la ER debe cerciorarse mediante la validación de la documentación e información requerida del solicitante del certificado que tanto el nombre del titular como del suscriptor correspondan a los solicitantes.
La ER tiene el derecho de rechazar una solicitud de certificado a causa de conflicto de nombres.

Documento de uso interno. Su contenido es confidencial y está destinado exclusivamente al personal autorizado de BIGDAVI S.A.C. Queda prohibida su reproducción, distribución o divulgación sin la autorización expresa de la Gerencia.

8.2. Validación inicial de la identidad

8.2.1. Método para probar la poseción de la clave privada

Si una EC ligada a la ER de BIGDAVI S.A.C. establece en su CPS o CP que el par de claves sea generado en las instalaciones de la ER, ésta debe demostrar la posesión de la clave privada, en virtud del procedimiento fiable de emisión, de entrega y de aceptación del dispositivo seguro, del correspondiente certificado y el par de claves almacenados en su interior, conforme a lo estipulado en la CPS de la EC.

8.2.2. Autenticación de la identidad de una persona jurídica

El proceso de comprobación de la identidad de la persona jurídica cuyos datos se incluyen en un certificado tiene como objetivo garantizar que el suscriptor y el titular sean las mismas personas identificadas en la solicitud de emisión de un certificado, y que la información que se incluya en el certificado sea verdadera y exacta. Para ello, la ER debe requerir al solicitante del certificado, presentarse personalmente, llevando la documentación establecida en su RPS. El personal asignado por la ER, deberá validar la identidad del solicitante, para ello la ER debe establecer los procedimientos de validación considerando los requerimientos sustentatorios establecidos por INDECOPI:

- El Representante Legal o una persona asignada por él deberá acreditar la existencia de la persona jurídica y su vigencia mediante los instrumentos públicos o norma legal respectiva, así como sus facultades como representante. Para ello, es preciso presentar un documento público o escritura que acredite dicha representación.
- La existencia y vigencia de la persona jurídica deberá acreditarse con el documento de vigencia respectivo expedido por los Registros Públicos o mediante la especificación de la norma legal de creación de la persona jurídica correspondiente. 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.
- El Representante Legal de la persona jurídica o una persona asignada por él, deberá firmar un contrato, que en adelante llamaremos “contrato del titular”. A través de dicho contrato, el titular deberá declarar tener conocimiento de los términos y condiciones aplicables a los certificados. La celebración de dicho contrato deberá realizarse antes de la emisión de los certificados.
- Si fuera el caso, los responsables de realizar las solicitudes de certificados, en representación de la persona jurídica, deben enviar las solicitudes a través de medios no repudiables, según lo establecido en su RPS.
- Los aspirantes a suscriptores deben presentarse a la ER. El proceso de verificación de sus identidades debe cumplir los requerimientos establecidos en el presente documento respecto de la autenticación de personas naturales.
- Tratándose de certificados digitales solicitados por personas jurídicas para su utilización a través de agentes automatizados, se deberá acreditar la existencia de la persona jurídica y la identidad de la persona responsable sobre dicho agente automatizado. La titularidad de certificados 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.
- Las ECs y ERs pueden ser titulares de certificados digitales, y deben ser tratados como personas jurídicas.

Documento de uso interno. Su contenido es confidencial y está destinado exclusivamente al personal autorizado de BIGDAVI S.A.C. Queda prohibida su reproducción, distribución o divulgación sin la autorización expresa de la Gerencia.

- La información proporcionada por los solicitantes deberá ser validada por la ER a través de un mecanismo de consulta confiable, como es el caso de las bases de datos nacionales o registros públicos. En caso contrario, no se podrá continuar el proceso de registro del solicitante.
- La EC debe referenciar en sus CPS los procedimientos de autenticación de la identidad de una persona jurídica, descritos en la RPS de la ER de BIGDAVI S.A.C.

8.2.3. Autenticación de la identidad de persona natural

El proceso de comprobación de la identidad de la persona natural cuyos datos se incluyen en un certificado tiene como objetivo garantizar que el titular sea la misma persona identificada en la solicitud de emisión de un certificado, y que la información que se incluya en el certificado sea verdadera y exacta. Para ello, la ER debe requerir al solicitante del certificado, presentarse personalmente, llevando la documentación establecida en su RPS.
El personal asignado por la ER, deberá validar la identidad del solicitante, para
ello la ER establece procedimientos de validación de los requerimientos sustentatorios establecidos por INDECOPI:

- La ER debe verificar la identidad del solicitante mediante la verificación del original de un documento oficial de identidad, el mismo que deberá estar en vigor en la fecha de realización del proceso de registro. No se admitirán fotocopias u otro tipo de documento.
- La información proporcionada por los solicitantes deberá ser validada por la ER a través de un mecanismo de consulta confiable, como es el caso de las bases de datos nacionales o registros públicos. En caso contrario, no se podrá continuar el proceso de registro del solicitante. En el caso de ciudadanos peruanos, para el nivel de seguridad Medio se puede emplear la base de datos del RENIEC, y para el nivel de seguridad Medio Alto, el sistema de identificación biométrica AFIS del RENIEC.

La EC debe hacer referencia en sus CPS los procedimientos de autenticación de la identidad de una persona individual, descritos en la RPS de la ER de BIGDAVI S.A.C.

8.2.4. Información no verificada del suscriptor

De manera general, no debe incluirse en los certificados, información no verificada del suscriptor o el titular según sea el caso. La IOFE permite una excepción en el caso de la

dirección de correo electrónico del suscriptor. En este caso se debe comprobar que la dirección de correo electrónico que se incluye en el certificado es la que efectivamente desea incluir el solicitante. Pero, la ER no está obligada a comprobar ni la existencia de la cuenta de correo electrónico indicada por el solicitante, ni que la dirección sea única, ni su correcto funcionamiento, todo lo cual es responsabilidad del solicitante.

8.2.5. Validación de la autoridad

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

8.3. Identificación y autenticación para solicitudes de re-emisión de certificado

El proceso de re-emisión es opcional para las EC, por ello cada EC es libre de decidir si habilitará o no el proceso. La ER de BIGDAVI S.A.C. informará a los suscriptores que la habilitación del proceso dependerá de si dicha habilitación se encuentra establecida en la CPS de la EC que emitió el certificado.

Documento de uso interno. Su contenido es confidencial y está destinado exclusivamente al personal autorizado de BIGDAVI S.A.C. Queda prohibida su reproducción, distribución o divulgación sin la autorización expresa de la Gerencia.

8.3.1. Identificación y Autenticación para solicitudes de remisión de certificad os rutinaria

La re-emisión de certificado rutinaria 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 menor a un plazo máximo de un año.
Sólo los titulares de certificados pueden solicitar la re-emisión de certificados, tanto en el caso de personas naturales como personas jurídicas.

Los titulares deben presentar a la ER la solicitud de re-emisión, acompañada de los documentos requeridos por la ER, los cuales están claramente establecidos en su RPS.

En este proceso, no es obligatoria la presencia del titular en la ER.
Antes de aprobar la re-emisión el certificado con la nueva clave pública, la ER deberá comprobar que la información del titular y del suscriptor contenida en el certificado continúa siendo válida. Si cualquier información del titular o del suscriptor hubiere cambiado, se registrará adecuadamente la nueva información. El titular o su representante deben presentar documentos que respalden dichas modificaciones.

En los casos que el certificado del titular hubiera expirado o hubiera sido revocado, deberá seguirse el proceso para la emisión de un nuevo certificado y la validación de identificación inicial descrita en la sección 8.2 de este documento.
Sólo se podrá realizar una única re-emisión de certificado.
Luego de la expiración de un certificado re-emitido, deberá seguirse el proceso para la emisión de un nuevo certificado y la validación de identificación inicial descrita en la sección 8.2 de este documento.

8.3.2. Identificación y Autenticación para la re-emisión de certificado luego de la revocación

En el caso que el certificado del titular haya sido revocado, deberá seguirse el proceso de validación de identidad inicial, especificado en la sección 8.2 de este documento.

8.4. Identificación y autenticación para la solicitud de revocación

El suscriptor y el titular pueden solicitar a la EC o ER la revocación de su certificado a través de medios telemáticos utilizando un medio que garantice el no repudio, como un mensaje firmado con

un certificado válido, la autenticación a través de una frase secreta conocida sólo por el suscriptor del certificado, etc.
En el caso de solicitud presencial, la ER de BIGDAVI S.A.C. establece en su RPS el formato de la solicitud y los documentos que debe presentar el solicitante de revocación para todos los casos:

- Los suscriptores deben presentar en la ER su documento oficial de identidad.
- Un representante asignado por la persona jurídica puede solicitar la revocación de los certificados de la entidad, para ello debe presentar a la ER, documentos que acrediten dicha representación y la voluntad de dicha persona jurídica.
- La IOFE permite que un tercero (diferente de la EC, el suscriptor y el titular), pueda solicitar la revocación de un certificado. En este caso, el solicitante deberá presentar en la ER pruebas fehacientes del uso indebido del certificado de acuerdo a la ley vigente.
- La revocación puede ser también solicitada mediante una orden judicial, la cual debe ser recibida y procesada por la ER.

Documento de uso interno. Su contenido es confidencial y está destinado exclusivamente al personal autorizado de BIGDAVI S.A.C. Queda prohibida su reproducción, distribución o divulgación sin la autorización expresa de la Gerencia.

9. Requisitos operacionales del ciclo de vida de los certificados

El ciclo de vida de un certificado personal no debe exceder el periodo establecido por la IOFE, el mismo que será de máximo tres (3) años de acuerdo a la legislación vigente.

9.1. Solicitud del certificado

Los procedimientos de solicitud dependerán de lo establecido en la CP y CPS de cada EC a la que BIGDAVI S.A.C. se encuentra vinculada.

9.1.1. Habilitados para presentar la solicitud de un certificado

Una ER acreditada puede aceptar la solicitud de certificados a nombre de una EC también acreditada, siempre y cuando dichos procesos sean establecidos en la CPS de cada EC a la que BIGDAVI S.A.C. se encuentra vinculada.
La solicitud en el caso de personas naturales debe ser hecha por la misma persona que pretende ser titular del certificado o por un representante que cuente con facultades expresas para tales efectos otorgadas mediante poder. En este caso, el titular del certificado será el poderdante y corresponderá al apoderado la condición de suscriptor. El ámbito de utilización del certificado digital en este supuesto, se encontrará circunscrito y limitado a las facultades expresamente conferidas en el poder.
En el caso de personas jurídicas, se pueden solicitar certificados de atributo para ser usados por funcionarios y personal específico, incluso por el Representante legal. En este caso, se considera como aspirante a titular del certificado a la persona jurídica y dichas personas naturales vienen a ser los aspirantes a suscriptor. El solicitante deberá especificar en su solicitud el tipo de atributo al que corresponderá el certificado. Se debe diferenciar entre el representante legal de la persona jurídica, de los trabajadores que como parte de su cargo requieren de un certificado digital. La EC, INDECOPI y los potenciales usuarios de dichos certificados, deben ser advertidos del procedimiento necesario para confirmar la titularidad de tal atributo y cualquier limitación que pudiera existir en el uso del mismo.
En el caso que el certificado esté destinado para ser usado por un agente automatizado, la solicitud debe ser hecha por un representante designado por la persona jurídica dueña del dispositivo. En este caso, la titularidad del certificado y de las firmas digitales generadas a partir de dicho certificado corresponderá a la persona jurídica. La atribución de responsabilidad, para tales efectos corresponde al representante legal, que en nombre de la persona jurídica solicita el certificado digital

Se debe permitir que un suscriptor pueda 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.
Cada EC a la que BIGDAVI S.A.C. se encuentra vinculada, puede establecer limitaciones para la adquisición de sus certificados digitales, de acuerdo a la comunidad de usuarios que haya especificado en su CPS.

9.1.2. Proceso de solicitud y responsabilidades

El proceso de solicitud y las responsabilidades asumidas por el uso del certificado, dependerán de lo establecido en las CP y CPS de cada EC a la que BIGDAVI S.A.C. se encuentra vinculada.

9.2. Procesamiento de la solicitud de un certificado

9.2.1. Realización de las funciones de identificación y autenticación

La ER de BIGDAVI S.A.C. especifica en su RPS, como mínimo, los

Documento de uso interno. Su contenido es confidencial y está destinado exclusivamente al personal autorizado de BIGDAVI S.A.C. Queda prohibida su reproducción, distribución o divulgación sin la autorización expresa de la Gerencia.

siguientes procedimientos de verificación para la validación de la identidad de una persona jurídica, natural o una PSC:

a. Establecer el requerimiento de una entrevista presencial con el solicitante del certificado para la verificación de su identidad.
b. Establecer el lugar donde se realice la verificación.
c. Establecer la persona responsable de la verificación.
d. Establecer la documentación requerida por la ER para identificar a una persona según la siguiente clasificación:
    - Natural
    - Jurídica
    - Atributos
    - Dispositivo para agente automatizado
    - PSC
e. Establecer los mecanismos de seguridad que permitan la validación de la documentación presentada por el solicitante del certificado para cada uno de los casos presentados en la clasificación, los cuales pueden requerir la consulta de bases de datos de información nacional, registros públicos, o AFIS.

La EC reconocerá la información de identificación de los suscriptores de las solicitudes proporcionadas por la ER.

Si las solicitudes son remitidas de manera electrónica, la ER debe realizar el correspondiente proceso de identificación y dicha solicitud debe ser firmada digitalmente por la ER empleando para tales efectos una clave de un certificado emitido por la EC u otra autoridad que haya sido reconocida por INDECOPI.

9.2.2. Aprobación o rechazo de la solicitud de certificado

La solicitud debe ser rechazada si el solicitante no está capacitado para participar de la comunidad de usuarios de la IOFE, sea el caso de una persona natural o jurídica o si el resultado de la validación realizada por la ER fue negativo, conforme a lo establecido en este documento.

En caso que una solicitud sea aprobada por la ER, dicha entidad debe realizar lo siguiente:

- Comunicar a la EC su aprobación para la emisión del certificado. Para ello se deben implementar los mecanismos de seguridad necesarios para establecer una comunicación segura entre la EC y la ER durante el proceso de emisión del certificado y generación del par de claves.
- La ER debe requerir del suscriptor la firma de un contrato de conformidad personal de dichas responsabilidades, así como de conformidad por parte de los titulares en cuyo nombre actúa el suscriptor.

El contrato antes aludido, deberá contener las obligaciones que deben cumplir los suscriptores y titulares de conformidad con la legislación de la materia, para garantizar el efecto legal de las transacciones realizadas empleando un certificado emitido por dicha EC, así como las consecuencias de no cumplir con el acuerdo.

Las ECs con las que BIGDAVI S.A.C. esté vinculada deben establecer el contenido del contrato del suscriptor en coordinación con esta ER, reflejando tanto las responsabilidades de la EC, la ER y la de los suscriptores y titulares; y los procedimientos a seguir para realizar la firma del mismo.

El contrato del suscriptor puede ser firmado de manera digital o manuscrita y debe ser archivado por la ER. El suscriptor debe firmar este documento incluso cuando la generación y la recepción del certificado son realizadas en la ER.

La ER debe registrar y archivar toda la documentación proporcionada por los solicitantes, lo cual incluye el contrato de suscriptor.

Documento de uso interno. Su contenido es confidencial y está destinado exclusivamente al personal autorizado de BIGDAVI S.A.C. Queda prohibida su reproducción, distribución o divulgación sin la autorización expresa de la Gerencia.

9.2.3. Tiempo para el procesamiento de la solicitud de un certificado

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

Las ECs con las BIGDAVI S.A.C. esté vinculada debe establecer en su CP u otra documentación relevante el tiempo necesario para el procesamiento de solicitudes, este tiempo no debe ser mayor a 5 días útiles a partir de la entrevista presencial del solicitante en la ER, considerando el intercambio de información necesario entre la EC y la ER.

9.3. Re-emisión de certificado

La ER de BIGDAVI S.A.C., en su RPS, indica que la ejecución del proceso de reemisión de certificados dependerá de cada EC a la que se encuentra vinculada.

9.3.1. Circunstancias para la re-emisión de un certificado

La IOFE permite el proceso de re-emisión de certificados. Las ECs a las que BIGDAVI S.A.C. se encuentra vinculada, que deseen ejecutar este proceso deben generar un nuevo par de claves y un nuevo certificado correspondiente a una nueva clave pública, pero manteniendo la mayor parte de la información del suscriptor contenida en el certificado a expirar, de acuerdo con lo establecido en este documento. Este nuevo certificado deberá ser actualizado en el Directorio de certificados emitidos del Repositorio para ser accesible a los terceros que confían y otras infraestructuras que reconozcan a la IOFE.

La re-emisión de claves rutinaria es un proceso programado cada vez que un nuevo par de claves debe ser emitido debido a su expiración y con anticipación a ésta. Siempre que una EC vinculada a BIGDAVI S.A.C. opte por brindar el servicio de re-emisión de certificados, la ER deberá permitir a los titulares solicitar una re-emisión rutinaria del mismo, antes de que ocurra la expiración de su certificado, siempre y cuando el periodo de vigencia de su certificado no sea mayor al plazo máximo de un año.

En el caso que el certificado del titular haya expirado o haya sido revocado, deberá seguirse el proceso de identificación inicial ante la ER, descrito en la sección 8.2 del presente documento.

Sólo se puede realizar una única re-emisión del certificado por un año adicional como máximo.

Importante: Tal y como se refleja en el contrato del suscriptor, a partir de la fecha en que el certificado expira, el suscriptor no podrá utilizar válidamente ni el certificado ya expirado, ni su clave privada.

Nota: En este proceso INDECOPI no exige la presencia personal del solicitante en la ER.

9.3.2. Personas habilitadas para solicitar la reemisión de certificado

Sólo el titular de un certificado puede solicitar la reemisión de su certificado, salvo que el certificado asociado a dicho par de claves estuviera revocado o hubiera superado el plazo máximo de vigencia de un año. Cuando el periodo de vigencia del certificado haya superado el plazo máximo de un año, deberá seguirse el proceso inicial de identificación descrito en la sección 8.2 del presente documento. La ER de BIGDAVI S.A.C. establece en su RPS los procedimientos necesarios para realizar la solicitud de re-emisión de certificado.

Nota: La ER de BIGDAVI S.A.C. únicamente aceptará solicitudes de re-emisión de certificados en representación de las ECs acreditadas, con las cuales mantiene un convenio para la prestación de servicios de certificación digital.

Documento de uso interno. Su contenido es confidencial y está destinado exclusivamente al personal autorizado de BIGDAVI S.A.C. Queda prohibida su reproducción, distribución o divulgación sin la autorización expresa de la Gerencia.

9.3.3. Procesamiento de las solicitudes para re-emisión de certificados

La solicitud de re-emisión de certificado debe ser rechazada en caso que el periodo de uso del certificado o las claves haya expirado o sea mayor a un año, en este caso deberá seguirse el proceso inicial de verificación de identificación ante la ER.
Antes de aprobar la re-emisión de un certificado, la ER deberá comprobar que la información utilizada para verificar la identidad y los restantes datos del titular y del suscriptor continúan siendo válidos. Si cualquier información del titular o del suscriptor ha cambiado, se debe registrar adecuadamente la nueva información.
La ER de BIGDAVI S.A.C. establece en su RPS los procedimientos necesarios para validar la información proporcionada por el solicitante de la re-emisión, su procesamiento y la posterior autorización o negación de la solicitud.
Luego de la verificación de los datos del titular y el suscriptor cuyos certificados se desean re•emitir, la ER deberá comunicar a la EC la aprobación de la solicitud.
La EC debe especificar en su CPS el mecanismo que la ER utilizará para comunicar la autorización de un proceso de re-emisión de un certificado, luego de la validación de la información.
La solicitud de re-emisión debe ser firmada por el solicitante de manera digital o manuscrita para garantizar el no repudio. Una copia de dicha solicitud firmada debe ser enviada a la EC.
La ER de BIGDAVI S.A.C. indica en su RPS que la ejecución del proceso de reemisión de certificados dependerá de cada EC a la que se encuentra vinculada.
La EC debe especificar en su CPS el mecanismo que la ER utilizará para comunicar la autorización de un proceso de re-emisión de un certificado, luego de la validación de la información.

9.4. Revocación y suspensión del certificado

9.4.1. Circunstancias para la revocación

La ER de BIGDAVI S.A.C. especifica en su RPS, las circunstancias
en las que los suscriptores, titulares o terceros pueden solicitar la revocación de un certificado, en las instalaciones de la ER. Como mínimo, el titular y el suscriptor del certificado están obligados, bajo responsabilidad, a solicitar la revocación al tomar conocimiento de la ocurrencia de alguna de las siguientes circunstancias:

- 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 sus representantes legales o apoderados.
- 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 contrato del suscriptor y/o titular.
- Cuando la información contenida en el certificado ya no resulte correcta.
- Por decisión de la legislación respectiva.

NOTA: En caso de cambios menores respecto a la información del titular que no tengan mayor impacto en los terceros que confían, puede no ser necesaria la revocación del certificado existente ni la emisión de uno nuevo.

Documento de uso interno. Su contenido es confidencial y está destinado exclusivamente al personal autorizado de BIGDAVI S.A.C. Queda prohibida su reproducción, distribución o divulgación sin la autorización expresa de la Gerencia.

9.4.2. Personas habilitadas para solicitar la revocación

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

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

9.4.3. Procedimiento para la solicitud de revocación

El suscriptor y el titular pueden solicitar a la EC o ER la revocación de su certificado a través de medios telemáticos utilizando un medio que garantice el no repudio, como un mensaje firmado con un certificado válido, la autenticación a través de una frase secreta conocida sólo por el suscriptor del certificado, etc.
Las ECs vinculadas a BIGDAVI S.A.C. debe establecer en su CPS, el procedimiento para realizar las solicitudes de revocación de los certificados de los suscriptores, emitidos por ECs acreditadas. El suscriptor también puede realizar la solicitud a la ER mediante una petición presencial.
Los terceros (incluyendo órdenes judiciales) deben presentarse personalmente o mediante un representante legalmente autorizado en las instalaciones de la ER para realizar la solicitud de revocación, con la documentación requerida. Dicha documentación y el proceso de validación de identidad del solicitante se encuentra especificado en la sección 8.2.
Una vez aprobada la solicitud de revocación, la ER deberá comunicar dicha aprobación a la EC correspondiente, dentro del plazo establecido por la EC, según los mecanismos establecidos en su CPS.
La CPS de la EC debe hacer referencia a las secciones competentes de la RPS de la ER, en lo correspondiente a la verificación de la identidad del solicitante de la revocación y su procesamiento, en los casos que la solicitud sea realizada en la ER. Además, debe establecer el procedimiento necesario para que la ER pueda enviar a la EC la autorización de revocación de un certificado.
Una EC puede revocar los certificados que ha emitido, siempre y cuando los motivos de revocación estén claramente especificados en su CPS y se encuentren de acuerdo con la legislación vigente.
Cuando una EC o ER recibe una solicitud para la revocación de un certificado, debe dejar 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 la misma a la EC, sus suscriptores y los terceros que confían. Las solicitudes deben ser firmadas de manera manuscrita o digital por los solicitantes.
En caso que no se acepte la revocación, deberá dejarse constancias de los hechos que motivaron dicha denegatoria.
Las responsabilidades del suscriptor que solicita una revocación de su certificado, deben estar claramente establecidas en el contrato del suscriptor.

9.4.4. Circunstancias para la suspensión

Las ECs vinculadas a BIGDAVI S.A.C. que deseen implementar el proceso de suspensión, deben indicarlo en su respectiva CPS, referenciando las secciones competentes de la RPS de la ER de BIGDAVI S.A.C. que especifica los procedimientos necesarios para la solicitud, procesamiento y consiguiente autorización o negación de una suspensión. Se indica en la RPS que la ejecución de este proceso dependerá de si se encuentra habilitado en la CPS de cada EC vinculada.

Documento de uso interno. Su contenido es confidencial y está destinado exclusivamente al personal autorizado de BIGDAVI S.A.C. Queda prohibida su reproducción, distribución o divulgación sin la autorización expresa de la Gerencia.

Sólo se puede solicitar la suspensión para el caso de personas jurídicas, cuando el suscriptor se ve impedido temporalmente de cumplir con sus funciones.

9.4.5. Personas habilitadas para solicitar la suspensión

Sólo los titulares de certificados emitidos a personas jurídicas pueden solicitar la suspensión de los certificados de sus suscriptores.

9.4.6. Procedimiento para la solicitud de la suspensión

Los titulares de certificados emitidos a personas jurídicas, pueden solicitar la suspensión de su certificado a la ER, a través de un representante legalmente autorizado.
El solicitante debe especificar las fechas de inicio y fin del periodo de suspensión.
El responsable de la ER debe requerir del solicitante, la firma manuscrita o
firma digital con certificado de atributos del representante en la solicitud de suspensión, la cual debe quedar registrada en la ER.
El certificado suspendido recobrará automáticamente su validez al término del periodo de suspensión solicitado por el titular.
La ER de BIGDAVI S.A.C. especifica, en su RPS, los procedimientos necesarios para la solicitud, procesamiento y consiguiente autorización o negación de una suspensión.

9.4.7. Límite del periodo de suspensión

El tiempo máximo en el que un certificado puede ser suspendido está limitado por su periodo de expiración.

10. Controles de las instalaciones, de la gestion y controles operacionales

10.1. Controles físicos

10.1.1. Ubicación y construcción del local

La ubicación y diseño del local debe prevenir, en lo razonablemente posible, el daño por desastres naturales, como inundación, terremoto; así como desastres creados por el hombre, como incendios, disturbios civiles y otras formas de desastre.
Se debe diseñar e implementar protección física en las oficinas y habitaciones, medios que garanticen la seguridad física de los equipos y del personal.
Se deben utilizar perímetros de seguridad (barreras tales como paredes y puertas de ingreso controlado o recepcionistas) para proteger las áreas que contienen información y medios de procesamiento de información. El acceso a las oficinas de registro público debe estar separado de las áreas que albergan los archivos y equipos que los PSCs utilizan para el procesamiento de la información sensible, de tal forma que únicamente el personal autorizado pueda acceder a ellos.

No debe haber ambientes compartidos que permitan la visibilidad de las operaciones críticas del sistema de registro o verificación. Estas operaciones deberán ser realizadas en compartimientos cerrados, que no permitan la visibilidad desde el exterior y que se encuentren físicamente protegidos.

10.1.2. Acceso físico

Se deben proteger las áreas sensibles mediante controles de acceso apropiados para garantizar que sólo se permita el acceso al personal autorizado.

Documento de uso interno. Su contenido es confidencial y está destinado exclusivamente al personal autorizado de BIGDAVI S.A.C. Queda prohibida su reproducción, distribución o divulgación sin la autorización expresa de la Gerencia.

Se deben controlar los puntos de acceso como las áreas de entrega, descarga y las áreas donde pueden ingresar personas no autorizadas.
Adicionalmente, debe llevarse un registro del acceso a áreas no públicas. Antes de otorgar acceso a áreas no públicas, se debe verificar la identidad de los visitantes, incluyendo a contratistas y personal de limpieza.
Se debe tomar en consideración el verificar los antecedentes de los visitantes, cuando sea factible realizar tal verificación.
Se debe identificar a los visitantes, como tales y de ser el caso, deberán de ser escoltados.

10.1.3. Energía y aire acondicionado

El equipo de energía y aire acondicionado, incluyendo el equipo de seguridad de los mismos, deben estar protegidos y en constante mantenimiento a efectos de asegurar su correcto funcionamiento.

10.1.4. Exposición al agua

Las instalaciones deben estar protegidas contra exposiciones al agua.

10.1.5. Prevención y protección contra fuego

Las instalaciones deben poseer adecuadas medidas para la prevención y protección contra el fuego.

10.1.6. Archivo de material

Los archivos tanto electrónicos como de papel y el material en general, debe estar protegido contra accesos no autorizados y destrucción tanto deliberada como accidental, incluyendo destrucción por fuego, temperatura, agua, humedad y magnetismo.
Los soportes de información sensible se deben almacenar de forma segura en armarios contra fuegos y cajas fuertes, según el tipo de soporte y la clasificación de la información en ellos contenida. Estos armarios deben situarse en diversas dependencias para eliminar riesgos asociados a una única ubicación.
El acceso a estos soportes debe estar restringido a personal autorizado.

10.1.7. Gestión de residuos

Se debe adoptar una política de gestión de residuos que permita la destrucción de cualquier tipo de material (físico o papel) que pudiera contener información, garantizando la imposibilidad de recuperación de esta información.

10.1.8. Copia de seguridad externa

Se deben disponer de copias de respaldo o de seguridad externa de toda la información sensible y de aquella considerada como necesaria para la persistencia de su actividad.
Las copias de seguridad externa deben ser establecidas y mantenidas de conformidad con las políticas de archivo y el plan de contingencias.

10.2. Controles procesales

10.2.1. Roles de confianza

Se deben definir los roles de confianza en las operaciones que se realizan en el interior del esquema de la ER.
La descripción de los roles debe incluir las labores que pueden como las que no pueden ser realizadas en el ejercicio de tales roles, las mismas que deben ser puestas de manifiesto a las personas que ejercen dichas funciones. Se debe obtener constancia por escrito del conocimiento de las mismas.

Documento de uso interno. Su contenido es confidencial y está destinado exclusivamente al personal autorizado de BIGDAVI S.A.C. Queda prohibida su reproducción, distribución o divulgación sin la autorización expresa de la Gerencia.

10.2.2. Número de personas requeridas por labor

Se debe identificar las labores que requieren de más de una persona para su realización.

10.2.3. Identificación y autenticación para cada rol

Deben emplearse controles de acceso tanto físicos como lógicos para verificar la identidad y autorización antes de permitir el acceso para cada rol.
El acceso a las comunicaciones con la EC o al sistema de Registro que permite leer, modificar o controlar los procesos del ciclo de vida de los certificados debe ser controlado por biometría o tarjeta inteligente.
Los operadores de registro, que tengan acceso para comunicar a la EC las aprobaciones a las solicitudes de emisión, revocación, modificación, suspensión o re-emisión de certificados digitales deben ser autenticados por medios biométricos o tarjeta inteligente.
El acceso a las bases de datos de la ER, que permiten la lectura y/o modificación de la información privada de los usuarios debe ser controlado por biometría o tarjeta inteligente.

10.2.4. Roles que requieren funciones por separado

Se deben definir los roles que requieren separación de funciones.
Las personas que se encargan de la implementación de una función, no deben asimismo tener el rol de realización de la auditoría de conformidad, o evaluación o revisión de dicha implementación.
También pueden ser identificadas otras áreas en las que potencialmente pueda existir conflicto.

10.3. Controles de personal

La ER de BIGDAVI S.A.C. establece, en su RPS u otra documentación relevante, los términos de confidencialidad y provisiones de no revelación que gobierna al mismo, así como la legislación que rige a las transacciones que se realizan bajo el marco de la IOFE, la legislación relativa al régimen de los trabajadores y cualquier otra legislación relevante, de conformidad con la Norma Marco sobre Privacidad.
Esta información debe ser entregada por escrito a empleados y contratistas, debiéndose obtener declaración por escrito por parte de estas personas respecto al de conocimiento de toda esta información.
Esta información debe ser incorporada en todos los contratos de trabajo o servicio.

10.3.1. Cualidades y requisitos, experiencia y certificados

La ER de BIGDAVI S.A.C. establece, en su RPS u otra documentación relevante, las cualidades, experiencias y certificados que deben poseer su personal y contratistas.

10.3.2. Procedimiento para verificación de antecedentes

Se deben verificar los antecedentes de todos los candidatos a empleados, contratistas y terceros en concordancia con las leyes vigentes y normatividad pertinente. La precisión de la verificación debe ser proporcional a los requerimientos comerciales, la clasificación de la información a la cual dicho personal tiene acceso y a los riesgos implicados.
Las personas que desempeñan roles de confianza deben de tener en claro el nivel de sensibilidad y valor de los bienes y transacciones protegidos por la actividad de la cual ellas son responsables.
Generalmente, esto involucra la verificación de la identidad de estas personas, cualidades y referencias, verificación de antecedentes criminales, verificación de antecedentes financieros, de crédito o similares, dentro de los límites legalmente establecidos en materia de privacidad.

Documento de uso interno. Su contenido es confidencial y está destinado exclusivamente al personal autorizado de BIGDAVI S.A.C. Queda prohibida su reproducción, distribución o divulgación sin la autorización expresa de la Gerencia.

10.3.3. Requisitos de capacitación

Todos los empleados de la organización (y cuando sea relevante los contratistas y terceros), deben recibir las capacitaciones apropiadas y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral.
La ER de BIGDAVI S.A.C. establece, en su RPS u otra documentación relevante, los requisitos de capacitación para su personal y contratistas.
Como mínimo, se debe incluir:

- El equipo y software requerido para operar.
- Los aspectos de la RPS, Política de Seguridad, Plan de privacidad y otra documentación relevante que afecte sus funciones.
- Requisitos legislativos en relación a sus funciones.
- Sus roles en relación al plan de contingencias.

10.3.4. Frecuencia y requisitos de las re•capacitaciones

Como mínimo las re•capacitaciones deben ser llevadas a cabo cuando existan cambios significativos en los elementos tratados en la capacitación inicial y cada vez que se sustituya o rote al personal encargado.

10.3.5. Frecuencia y secuencia de la rotación en el trabajo

La ER de BIGDAVI S.A.C. establece en su RPS u otra documentación relevante si implementará políticas de rotación en el trabajo,
en ese caso se debe establecer documentalmente los procedimientos necesarios, incluyendo los periodos mínimos para realizar la rotación.

10.3.6. Sanciones por acciones no autorizadas

Debe existir un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad. Como mínimo, en el caso de una acción real o potencial no autorizada y que haya sido realizada por una persona que desempeña un rol de confianza, dicha persona debe ser inmediatamente suspendida de todo rol de confianza que pudiera desempeñar.
Dichas sanciones deben estar establecidas en los contratos de cada empleado y/o contratista.

10.3.7. Requerimientos de los contratistas

Se debe establecer en la RPS u otra documentación relevante, si es que se permite el empleo de contratistas.
Los contratistas y su personal deben quedar obligados por los términos de la RPS y otra documentación relevante de la IOFE que les afecte.
Los contratos deben especificar sanciones y reparaciones para las acciones llevadas a cabo por los contratistas y sus empleados.

10.3.8. Documentación suministrada al personal

Se debe entregar al personal la documentación necesaria para el desempeño
de sus funciones. Como mínimo, esto debe incluir:

- Una declaración de funciones y autorizaciones.
- Manuales para los equipos de software que deben de operar.
- Aspectos de la RPS, política de seguridad y otra documentación relevante en relación a sus funciones.
- Legislación aplicable a sus funciones.

Documento de uso interno. Su contenido es confidencial y está destinado exclusivamente al personal autorizado de BIGDAVI S.A.C. Queda prohibida su reproducción, distribución o divulgación sin la autorización expresa de la Gerencia.

- Documentación respecto a sus roles frente a plan de contingencia.

10.4. Procedimiento de registro de auditorías

10.4.1. Tipos de eventos registrados

Se debe mantener un registro de auditoría de los eventos que puedan impactar en la seguridad de sus operaciones.
Como mínimo, estos deben incluir lo siguiente:

- Encendido y apagado de los sistemas que procesan información sensible.
- Intentos de crear, borrar, cambiar contraseñas o permisos de los usuarios dentro del sistema que procesa información sensible.
- Intentos de entrada y salida del sistema que procesa información sensible.
- Intentos no autorizados de acceso a los registros o bases de datos del sistema.
- Se debe registrar de manera manual o electrónica, la siguiente información:
- Mantenimientos y cambios de configuración del sistema que procesa información sensible.
- Acceso físico a las áreas sensibles.
- Cambios en el personal.
- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte al sistema de certificación.

El registro de auditoría de eventos debe registrar la hora, fecha e identificadores de software/hardware.

10.4.2. Frecuencia del procesamiento del registro

Los registros de auditoría deben ser procesados y revisados una vez al mes como mínimo con el fin de buscar actividades sospechosas o no habituales. Los eventos auditables significativos deben generar alarmas automáticas para realizar una auditoría.
El procesamiento de los registros de auditoría debe incluir la verificación de que dichos registros no hayan sido manipulados.

10.4.3. Periodo de conservación del registro de auditorías

Como mínimo el registro de auditorías debe conservarse por un periodo de diez (10) años, el cual es el periodo máximo requerido por la jurisdicción con la cual la IOFE mantiene un acuerdo de reconocimiento cruzado.

10.4.4. Protección del registro de auditoría

Los archivos donde se almacene la información relevante para las auditorías deben estar protegidos por listas de control de acceso que permitan solamente a los administradores de la ER tener acceso a esa información tanto para lectura, como para escritura.

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.

10.4.5. Procedimiento de copia de seguridad del registro de auditorías

Como mínimo debe realizarse de manera mensual una copia de seguridad del registro de auditorías, la cual debe archivarse fuera de sus instalaciones.
Debe tomarse en consideración la posibilidad de generar copias de seguridad automatizadas para el caso de eventos auditables significativos.

Documento de uso interno. Su contenido es confidencial y está destinado exclusivamente al personal autorizado de BIGDAVI S.A.C. Queda prohibida su reproducción, distribución o divulgación sin la autorización expresa de la Gerencia.

10.4.6. Sistema de realización de auditoría (Interna vs Externa)

Las auditorías internas deben llevarse a cabo, como mínimo, una vez al año en la ER.
Las evaluaciones técnicas (auditorías externas) se llevarán llevarse a cabo una vez al año (auditoría periódica).
Las visitas comprobatorias serán llevadas a cabo siempre que INDECOPI lo requiera, después de pasados los tres (3) primeros meses de funcionamiento de la ER.

10.4.7. Notificación al titular que causa un evento

Se debe establecer en la RPS de la ER u otra documentación relevante si es que resulta factible realizar notificaciones a los titulares que causan los eventos. Debe tomarse en consideración la posibilidad de permitir la notificación a un titular en los casos en que se establezca que el evento es de índole accidental y resulta probable que pueda volver a ocurrir.

10.4.8. Valoración de vulnerabilidad

Se debe establecer en la RPS u otra documentación relevante, los procedimientos para la valoración de la vulnerabilidad de los sistemas y de ser el caso, la frecuencia en que la misma debe realizarse.

10.5. Archivo de registro

10.5.1. Tipos de eventos registrados

Como mínimo deben mantenerse: los datos de los suscriptores y titulares, los contratos y documentos que dan constancia de cada solicitud realizada en la ER, las claves públicas de dicha entidad y el registro de auditorías.

10.5.2. Periodo de conservación del archivo

El periodo de conservación de los archivos. Como mínimo, los archivos deben ser mantenidos por un periodo de diez (10) años, el cual es el periodo máximo requerido por la legislación vigente.
Las aplicaciones requeridas para tener acceso a un archivo deben también ser archivadas.

10.5.3. Protección del archivo

Se debe establecer en la Política de Seguridad u otra documentación relevante las medidas de protección de la información archivada. Como mínimo las medidas deben prevenir cualquier modificación o eliminación de los datos contenidos en el archivo, e impedir el acceso a personas no autorizadas. Asimismo, debe garantizarse la confidencialidad de los datos proporcionados por los suscriptores y los titulares. Las medidas de seguridad que se adopten deben ser proporcionales a la sensibilidad e importancia de la información contenida en el archivo.
Los archivos de mayor relevancia, así como los certificados digitales deben estar firmados digitalmente.

Debe tomarse en consideración la posibilidad de re•firmado de los archivos cuando los avances en las tecnologías generen potencialmente una posibilidad de afectación a los mismos o la generación de microformas según Decreto Legislativo 681.

10.5.4. Procedimientos para copia de seguridad del archivo

Con el fin de mantener la integridad y disponibilidad de los servicios de procesamiento de información y comunicaciones, se deben realizar copias de respaldo de la información y software esencial. Dichas copias deben ser probadas con regularidad. Los procedimientos deben ser compatibles con los estándares

Documento de uso interno. Su contenido es confidencial y está destinado exclusivamente al personal autorizado de BIGDAVI S.A.C. Queda prohibida su reproducción, distribución o divulgación sin la autorización expresa de la Gerencia.

ISO mencionados en las referencias de esta sección o la generación de microformas de acuerdo al Decreto Legislativo 681.

10.5.5. Requisitos para los archivos de sellado de tiempo

Los datos archivados deben consignar la fecha y hora, y la firma digital de la organización que genera dichos datos según la RFC 3161 (Time Stamping), o pueden ser protegidos de cualquier otra forma que pueda demostrar que los datos corresponden a la organización que los ha generado.

10.5.6. Sistema de recolección del archivo (Interna o Externa)

Se requiere que por lo menos se mantengan dos copias de seguridad, una de las cuales debe ser almacenada fuera de las instalaciones del mismo.

10.5.7. Procedimiento para obtener y verificar la información del archivo

Los procedimientos para la obtención y verificación de la información del archivo deben encontrarse de conformidad con los requisitos de confidencialidad y privacidad detallados en los puntos 13.3 y 13.4.

10.6. Recuperación frente al compromiso y desastre

Se establece un plan de contingencias que permita el restablecimiento y mantenimiento de las operaciones de la ER. Este plan debe contemplar las acciones a realizar, los recursos a utilizar y el personal a emplear en el caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos y los servicios de certificación.
Dicho plan debe asegurar que los aspectos básicos del negocio, tales como servicios de validación o revocación, puedan ser reasumidos dentro de un plazo máximo de 24 horas, el cual constituye el plazo máximo para la emisión de las listas de revocación de certificados. Los planes deben ser evaluados por lo menos una vez durante el periodo de cada auditoría o evaluación de compatibilidad y los resultados deben ser puestos a disposición de los auditores de compatibilidad o asesores, conjuntamente con la información respecto a las acciones correctivas que pudieran ser necesarias.

10.6.1. Procedimiento de manejo de incidentes y compromisos

El plan de contingencias debe establecer de manera específica los procedimientos que deben seguirse en el caso de un evento o compromiso real o potencial de la integridad de las operaciones de la ER. Los eventos e incidentes que afecten la seguridad de la información deben reportarse al Responsable de Seguridad lo más rápidamente posible.

Todos los empleados, contratistas y terceros que confían de los sistemas y servicios de información deben tomar nota y reportar al Responsable de Seguridad cualquier debilidad observada o sospechosa sobre la seguridad de dichos sistemas y servicios de información, con el fin de identificar dichos eventos y reducir el impacto de los mismos.

Cuando la acción de seguimiento contra una persona u organización después de un incidente en la seguridad de la información involucra una acción legal (civil o criminal), se debe recolectar, mantener presentar evidencia a fin de cumplir con la legislación vigente.

10.6.2. Adulteración de los recursos computacionales, software y/o datos

El plan debe identificar fuentes alternativas de recursos computacionales, software y datos, las cuales deben ser empleadas en los casos de adulteraciones o fallas en los mismos.

Documento de uso interno. Su contenido es confidencial y está destinado exclusivamente al personal autorizado de BIGDAVI S.A.C. Queda prohibida su reproducción, distribución o divulgación sin la autorización expresa de la Gerencia.

En el caso que la adulteración se refiera al compromiso real o potencial de las claves privadas que pudiera generar su inoperatividad, debe tomarse en consideración la posibilidad de realizar un proceso de reemisión.

10.6.3. Procedimientos en caso de compromiso de la clave privada de la entidad

En el caso de compromiso de la clave privada de un empleado que cumpla un rol de confianza, el certificado deberá ser revocado y se deberá solicitar la emisión de un nuevo certificado.

10.7. Finalización de la EC o ER

Se requiere información por parte de los PSCs respecto a operaciones de finalización (disolución) o transferencia de su titularidad. La ER debe informar 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.

Cuando un PSC finaliza sus operaciones, se debe asegurar que todos los datos necesarios para la continuación de las operaciones bajo el marco de la IOFE son transferidos al propio INDECOPI o a otro PSC designado por éste.

Cuando se trata de una operación de transferencia de titularidad, se debe asegurar que los nuevos dueños u operadores cumplan con los requisitos de acreditación.

Se debe advertir a todos los suscriptores o 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.

11. Controles de seguridad técnica

11.1. Generación e instalación del par de claves

11.1.1. Generación del par de claves

La generación de claves tanto para uso de INDECOPI, los PSCs como para uso de los usuarios finales, debe ser realizada utilizando procedimientos de generación de claves compatibles con el estándar FIPS 140-2 Sección 4.7.2 o Common Criteria EAL4+ como mínimo.

Las claves pueden ser generadas por los propios suscriptores o por las ERs.

11.1.2. Entrega al suscriptor de la clave privada

En el caso que la ER genere las claves a nombre del suscriptor, deben implementarse controles que aseguren la confidencialidad de la clave privada asociada.

En los casos en que las claves no son emitidas en presencia del suscriptor o titular, se debe permitir la emisión electrónica de claves, proveyendo canales seguros por separado para la emisión de la clave y para el código (o códigos) de activación de la misma.

11.1.3. Entrega de la clave pública para el emisor de un certificado

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 la ER acepte 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.

Documento de uso interno. Su contenido es confidencial y está destinado exclusivamente al personal autorizado de BIGDAVI S.A.C. Queda prohibida su reproducción, distribución o divulgación sin la autorización expresa de la Gerencia.

11.2. Controles de ingeniería para protección de la clave privada y módulo criptográfico

11.2.1. Estándares y controles para el módulo criptográfico

Los módulos criptográficos usados por las ECs deben cumplir los requerimientos o ser equivalentes a FIPS 140•2, nivel de seguridad 3.
Los módulos criptográficos usados por la ER de BIGDAVI S.A.C. o eventuales Proveedores de servicios de repositorio acreditados (si fuesen requeridos) deben cumplir los requerimientos o ser equivalentes a los requerimientos de FIPS 140-2 nivel de seguridad 2 como mínimo.
Los módulos criptográficos usados por los titulares o suscriptores bajo el marco de la IOFE deben cumplir los requerimientos o ser equivalentes a los requerimientos de FIPS 140-2 nivel 1.
NOTA: Los requerimientos exigidos en esta sección se aplican tanto al hardware como al firmware (“sistema operativo”) de los módulos criptográficos.

11.2.2. Depósito de clave privada

No se admite el depósito, almacenamiento o copia de claves privadas de firma y autenticación de los usuarios finales, ni de los módulos hardware que los contienen.
Sólo se permitiría el depósito de claves privadas de cifrado (copia de back up), sólo si media consentimiento del suscriptor.

11.2.3. Archivo de la clave privada

No deberán ser archivadas las claves privadas empleadas para la firma y autenticación de los usuarios finales, ni de los archivos electrónicos que los contengan (por ejemplo, los archivos con extensión PFX o P12).
Otras claves privadas pueden ser archivadas a efectos de permitir la restauración del material correspondiente.
En los casos en que se archive una clave privada, ésta deberá ser protegida en el mismo nivel que se emplea para la protección de la clave activa.

11.2.4. Clasificación del módulo criptográfico

Los módulos criptográficos usados por las ECs o por las Autoridades de Gestión de ECs, deben cumplir los requisitos establecidos o que sean equivalentes a FIPS 140•2 nivel de seguridad 3 como mínimo.
Los módulos criptográficos usados por los ERs o por los Proveedores del Servicio de Repositorio acreditados deben cumplir los requisitos establecidos o que sean equivalentes a FIPS 140•2 nivel de seguridad 2 como mínimo.
Los módulos criptográficos usados por los suscriptores de certificados acreditados por la IOFE deben cumplir los requisitos establecidos o que sean equivales a FIPS 140•2 nivel de seguridad 1 como mínimo y según el nivel de seguridad medio y medio alto.

11.3. Datos de activación

11.3.1. Otros aspectos de los datos de activación

El ciclo de vida de los datos de activación debe de estar de conformidad con el valor de los activos protegidos por la clave privada. Como ejemplo, puede requerirse el cambio de PINs y contraseñas cada 30 días con limitaciones en cuanto a su formato y uso.

Documento de uso interno. Su contenido es confidencial y está destinado exclusivamente al personal autorizado de BIGDAVI S.A.C. Queda prohibida su reproducción, distribución o divulgación sin la autorización expresa de la Gerencia.

11.4. Controles de seguridad computacional

En caso que la ER de BIGDAVI S.A.C. mantenga o procese la información sensible en equipos informáticos, deberá considerar las siguientes sub-secciones.

11.4.1. Requisitos técnicos específicos para seguridad computacional

La ER de BIGDAVI S.A.C. establece en su RPS los controles de seguridad computacional, incluyendo métodos necesarios para la evaluación de dichos controles.

11.4.2. Evaluación de la seguridad computacional

Las evaluaciones deben ser realizadas de manera compatible con estándares internacionales.

12. Auditorias de compatibilidad y otras evaluaciones

Se debe estar sometido a auditoría de compatibilidad independiente en relación a las operaciones que realiza. La frecuencia de auditorías externas o evaluaciones de compatibilidad y el proceso de publicación de los resultados debe ser de una vez al año.
La auditoría de compatibilidad o los procesos de evaluación requeridos para obtener y mantener la acreditación debe asimismo estar establecidos en la RPS u otra documentación relevante.

12.1. Frecuencia y circunstancias de la evaluación

La ER de BIGDAVI S.A.C., se debe someter una vez al año a auditorías o evaluaciones de conformidad respecto del marco de la IOFE. También puede someterse a auditorías o evaluaciones de conformidad en relación a lo establecido en su RPS.
Se debe de publicar el resultado de estas auditorías o evaluaciones de compatibilidad.

12.2. Identidad/Calificaciones de asesores

Un equipo de auditoría o evaluación de compatibilidad debe incluir a personas con experiencia significativa en tecnologías de la información, seguridad y tecnologías de PKI y criptográficas.
INDECOPI exige que las personas que realizan las auditorías o evaluaciones de compatibilidad bajo el marco de la IOFE, sean previamente aprobadas por éste.

12.3. Relación del auditor con la entidad auditada

Los auditores o asesores deben ser independientes de la organización que auditan o evalúan.

12.4. Elementos cubiertos por la evaluación

Los elementos cubiertos por la auditoría son la implementación de las prácticas de personal, procedimientos y técnicas descritas en este documento. Entre los principales elementos donde se enfocará la auditoría son:

a) Identificación y autenticación.
b) Servicios y/o funciones operacionales.
c) Los controles de seguridad física.
d) Los controles para la ejecución de los procedimientos y los controles de personas que aplican para la ER.
e) Controles de seguridad técnicos.

Documento de uso interno. Su contenido es confidencial y está destinado exclusivamente al personal autorizado de BIGDAVI S.A.C. Queda prohibida su reproducción, distribución o divulgación sin la autorización expresa de la Gerencia.

12.5. Acciones a ser tomadas frente a resultados deficientes

Al detectarse una irregularidad, y dependiendo de la gravedad de la misma, podrán tomarse entre otras las siguientes acciones:

a) Indicar las irregularidades, pero permitir al PSC que continúe sus operaciones hasta la próxima auditoría programada.
b) Permitir al PSC que continúe sus operaciones por un máximo de treinta (30) días naturales pendientes a la corrección de los problemas antes de suspenderlo. c) Suspender la operación del PSC.

El auditor entregará a la AAC un informe técnico sustentando las acciones a realizar y la AAC determinará cuál de estas acciones deberá ser tomada.

12.6. Publicación de Resultados

Los resultados de las auditorías o evaluaciones de compatibilidad bajo el marco de la IOFE deben ser publicados como parte de la información de estado, la cual es publicada por INDECOPI.

13. Otras materias de negocio y legales

13.1. TARIFAS

Las tarifas a ser pagadas por participar de la IOFE deben estar de acuerdo a la legislación vigente.
Las ER de BIGDAVI S.A.C. en convenio con las ECs vinculadas, establecen el monto de sus tarifas. En particular, las tarifas deben ser referenciadas en los contratos de suscriptores y terceros que confían.

13.1.1. Tarifas para la emisión o renovación de certificados

La ER de BIGDAVI S.A.C. indica, en su RPS u otra documentación relevante, la información correspondiente a la ubicación de las tarifas a ser pagadas por este servicio. En particular, las tarifas deben estar establecidas o referenciadas en los contratos de suscriptores y terceros que confían.

13.1.2. Tarifas para otros servicios

La ER de BIGDAVI S.A.C. indica, en su RPS u otra documentación relevante, la información correspondiente a la ubicación de las tarifas a ser pagadas por este servicio. En particular, las tarifas deben estar establecidas o referenciadas en los contratos de suscriptores y terceros que confían.

13.1.3. Políticas de reembolso

La ER de BIGDAVI S.A.C., establece, en su RPS u otra documentación relevante, sus políticas de reembolso. En particular, las políticas deben estar establecidas o referencias en los contratos de suscriptores y terceros que confían.

13.2. Responsabilidad financiera

13.2.1. Cobertura de seguro

El monto mínimo de la póliza es fijada por la AAC.

Documento de uso interno. Su contenido es confidencial y está destinado exclusivamente al personal autorizado de BIGDAVI S.A.C. Queda prohibida su reproducción, distribución o divulgación sin la autorización expresa de la Gerencia.

13.2.2. Cobertura de seguro o garantía para entidades finales

En el caso que exista cobertura de seguro o garantía disponibles para los suscriptores, la ER de BIGDAVI S.A.C. debe establecer en su RPS los tipos correspondientes, lo cual deberá también ser referenciado en el contrato de suscriptor, incluyendo los términos y condiciones de dicha cobertura.
En el caso que exista cobertura de seguro o garantía disponibles para los terceros que confían, esto deberá encontrarse referenciado en la CPS, en donde deben incluirse los términos y condiciones de la cobertura para el tercero que confía.

13.3. Confidencialidad de la información del negocio

13.3.1. Alcances de la información confidencial

Se deben mantener de manera confidencial la siguiente información:

- Material comercialmente reservado de la ER, de los suscriptores de empresa y de las terceros que confían, incluyendo términos contractuales, planes de negocio y propiedad intelectual;
- Información que puede permitir a partes no autorizadas establecer la existencia o naturaleza de las relaciones entre los suscriptores de empresa y los terceros que confían; Información que pueda permitir a partes no autorizadas la construcción de un perfil de las actividades de los suscriptores, titulares o terceros que confían.
- Se debe asegurar la reserva de toda información que mantiene, la cual pudiera perjudicar la normal realización de sus operaciones.

Se permite la publicación de información respecto a la revocación o suspensión de un certificado, sin revelar la causal que motivó dicha revocación o suspensión.
La publicación puede estar limitada a suscriptores legítimos, titulares o terceros que confían.

13.3.2. Información no contenida dentro del rubro de información confidencial

Se debe permitir la publicación de certificados (siempre que el suscriptor lo autorice en el contrato del suscriptor) e información de estado de certificados, así como de información en relación a la revocación de un certificado sin revelar la razón de dicha revocación.
La publicación puede estar limitada a suscriptores legítimos, titulares o terceros que confían.

13.3.3. Responsabilidad de protección de la información confidencial

Se debe cumplir tanto los requisitos de confidencialidad como las leyes sobre protección de datos, confidencialidad de la información y propiedad intelectual que les fueren aplicables, tal y como está establecido en el Plan de Privacidad y la Norma Marco sobre Privacidad.

13.4. Privacidad de la información personal

Se debe cumplir con la legislación sobre protección de datos de conformidad con la Norma Marco sobre Privacidad.
También debe tomarse en consideración la legislación sobre protección de datos de las jurisdicciones con las que mantengan acuerdos de reconocimiento cruzado y las políticas de protección de datos personales existentes en dichas infraestructuras. Debe tomarse particular atención a las provisiones relativas a la transferencia internacional de información personal.
Se debe realizar evaluaciones de impacto a la privacidad de sus operaciones.

13.4.1. Plan de privacidad

Se requiere la preparación de un plan de privacidad de conformidad con la Norma Marco sobre Privacidad.

Documento de uso interno. Su contenido es confidencial y está destinado exclusivamente al personal autorizado de BIGDAVI S.A.C. Queda prohibida su reproducción, distribución o divulgación sin la autorización expresa de la Gerencia.

El plan debe establecer el tipo de datos personales que pueden ser recolectados y cómo serán utilizados, protegidos, recuperados/corregidos, las circunstancias en que estos serán revelados y las sanciones en caso de incumplimiento del plan.
NOTA: El contenido del plan, incluyendo las sanciones, puede impactar en la posibilidad de llevar a cabo transferencias internacionales de datos personales entre infraestructuras.

13.4.2. Información tratada como privada

Se debe mantener de manera confidencial la siguiente información:

- Información personal provista por los suscriptores, titulares y terceros que confían que no sea la autorizada para estar contenida en certificados y repositorios;
- Información que pueda permitir a partes no autorizadas establecer la existencia o naturaleza de las relaciones entre suscriptores, titulares y terceros que confían;
- Información que pueda permitir a partes no autorizadas la construcción de un perfil de las actividades de los suscriptores, titulares o terceros que confían.
- Se debe permitir la publicación de información respecto a la revocación o suspensión de un certificado, sin revelar la causal que motivó dicha suspensión o revocación.

La publicación puede estar limitada a suscriptores legítimos, titulares o terceros que confían.

13.4.3. Información no considerada privada

Se permite la divulgación de información personal sólo en los casos en que exista consentimiento expreso del individuo cuya información corresponde.

13.4.4. Notificación y consentimiento para el uso de información

En los contratos y acuerdos que serán firmados por los suscriptores se debe establecer el tipo de datos personales que pueden ser recolectados, cómo serán utilizados, protegidos y cómo estos pueden ser revisados/corregidos, las circunstancias bajo las cuales serán divulgados, la manera de desagravios y sanciones para las fallas en el cumplimiento del acuerdo con la parte o partes que utilizan o recolectan dichos datos. Asimismo, debe incorporarse en el acuerdo, el necesario consentimiento para la divulgación de datos específicos. Las notificaciones relevantes efectuadas a los terceros que confían deben establecer de manera específica los datos personales que pueden ser recolectados, cómo serán usados, protegidos y cómo pueden ser revisados/corregidos, las circunstancias bajo las cuales serán divulgados, la manera de desagravios y sanciones para las fallas en el cumplimiento del plan. De ser posible, deberá obtenerse consentimiento explícito para la revelación de datos específicos.
Cuando esto no sea posible, el tercero que confía debe ser informado que el
acceso al material implicará la dación de un consentimiento implícito con los términos antes señalados.

NOTA: El contenido del plan, incluyendo las sanciones, puede impactar en la posibilidad de llevar a cabo transferencias internacionales de datos personales entre infraestructuras.

13.4.5. Divulgación realizada con motivo de un proceso judicial o administrativo

Se debe permitir la revelación de información personal a oficiales encargados del cumplimiento de leyes o como parte de un descubrimiento civil, donde se hace una solicitud de conformidad con la ley aplicable en la jurisdicción en donde la ER se encuentra localizada.
Cuando la solicitud de divulgación de información proviene de otra jurisdicción, debe permitirse la aplicación de leyes de asistencia mutua.

Documento de uso interno. Su contenido es confidencial y está destinado exclusivamente al personal autorizado de BIGDAVI S.A.C. Queda prohibida su reproducción, distribución o divulgación sin la autorización expresa de la Gerencia.

13.4.6. Otras circunstancias para divulgación de información

Se debe permitir a los suscriptores, titulares y terceros que confían solicitar la divulgación de la información que han provisto a terceros.
Se debe requerir que la divulgación de la información bajo otras circunstancias se realice solamente de conformidad con la CP u otra documentación relevante y que esto se encuentra de conformidad con la ley aplicable y con la Norma Marco sobre Privacidad.

13.5. Derecho de propiedad intelectual

Se debe asegurar que el acceso necesario a información de registro, nombres, incluyendo copias de archivo, se encuentra disponible para INDECOPI a efectos de continuar las operaciones en el marco de la IOFE en el caso de eliminación o falla de la ER. Esto puede involucrar temas de propiedad intelectual.
La ER de BIGDAVI S.A.C. deberá mantener los derechos de propiedad intelectual necesarios para el material y procesos que utiliza para las operaciones dentro del marco de la IOFE.

13.6. Representaciones y garantías

13.6.1. Representaciones y garantías de la ER

La ER establece en su RPS provisiones de garantía y responsabilidad, incluyendo limitaciones y exclusiones. Debe asimismo asegurar que dichas provisiones se encuentran establecidas en los contratos de suscriptor y tercero que confía.
En particular, la ER establece responsabilidades 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.

13.6.2. Representaciones y garantías de los suscriptores

Un suscriptor o titular debe estar obligado a cumplir las obligaciones de suscriptor establecidas en el CP y CPS de la EC vinculada a la ER de BIGDAVI S.A.C.
Se debe requerir al suscriptor la firma de un acuerdo de cumplimiento de sus obligaciones, incluyendo las concernientes a los titulares inscritos por él. El acuerdo debe incluir las consecuencias de eventuales incumplimientos.
El acuerdo del suscriptor debe contemplar las obligaciones cuando la legislación las establezca a los suscriptores o titulares a fin de asegurar los efectos legales de las transacciones realizadas utilizando certificados emitidos por la EC.
Cuando una jurisdicción establece obligaciones a los suscriptores o titulares que se encuentran fuera de dicha jurisdicción, estas obligaciones deben de estar disponibles para los suscriptores o titulares.
Las obligaciones del suscriptor o titular pueden incluir una garantía de la exactitud de la información provista en las aplicaciones del certificado, acordando la protección de claves y certificados frente a malos usos y el acuerdo de no empleo de las claves y certificados fuera de los alcances de la IOFE.
Cuando un suscriptor celebra un acuerdo en representación de un número de titulares, sus responsabilidades en relación a las acciones de dichos titulares, también deben estar claramente establecidas.

13.6.3. Representaciones y garantías de las terceros que confían

Un tercero que confía puede ser requerido a cumplir con las obligaciones del tercero que confía establecidas en la RPS de la ER. Se le debe notificar al tercero que confía dichas obligaciones por intermedio de la publicación de un documento accesible para el tercero que confía. La declaración o documento, debe incluir las consecuencias derivadas del incumplimiento del acuerdo. Cuando la

Documento de uso interno. Su contenido es confidencial y está destinado exclusivamente al personal autorizado de BIGDAVI S.A.C. Queda prohibida su reproducción, distribución o divulgación sin la autorización expresa de la Gerencia.

legislación establezca determinadas obligaciones al tercero que confía para asegurar efecto legal a las transacciones realizadas utilizando certificados en los cuales esta parte confía, la documentación debe de establecer dichas obligaciones.
Las obligaciones del tercero que confía pueden incluir la necesidad de verificación del estado de los certificados y el acuerdo de no usar los certificados fuera de los términos establecidos en el marco de la IOFE.

13.6.4. Representaciones y garantías de otros participantes

Otros participantes no específicamente mencionados anteriormente, deben establecer en su declaración de prácticas u otra documentación provisiones sobre garantías y responsabilidades, incluyendo limitaciones y exclusiones de las mismas. Asimismo, deben asegurar que dichas provisiones se incluyan en todo contrato de suscriptor o tercero que confía.

13.7. Exención de garantías

La ER establecer en su RPS y otra documentación relevante, cualquier exención de responsabilidad que pudiera aplicársele.
Asimismo, se debe asegurar que estas provisiones sean incluidas en cualquier contrato de suscriptor o tercero que confía.
No cabe exención de responsabilidad para aquellas garantías establecidas por la legislación vigente.

13.8. Indemnizaciones

La ER debe establecer en su RPS y otra documentación relevante lo relativo a las indemnizaciones a las que pudieran estar sujetos.
Asimismo, debe asegurar que estas provisiones sean incluidas en cualquier contrato de suscriptor o tercero que confía o documentación.

13.9. Término y terminación

13.9.1. Término

El periodo de validez máximo de la documentación relativa a la ER es de tres (3) años, de acuerdo a la legislación vigente.
Cuando caduca la acreditación de la ER, su documentación también debe de caducar. Cuando la ER opera tanto dentro como fuera del marco de la IOFE, el término y la terminación sólo debe referirse a la documentación relativa a la IOFE.
El término de validez de la documentación de la ER debe estar sujeto a la continuidad de la acreditación.
En el caso que un PSC opere tanto dentro como fuera de la IOFE, el término y la terminación debe referirse sólo a documentación relativa a la IOFE.
Se permite que los contratos de suscriptor y tercero que confía sean culminados cuando las partes del acuerdo incumplen sus obligaciones dentro del marco de la IOFE.
La ER deberá modificar dicha documentación cada vez que INDECOPI y/o la misma entidad lo determine.

13.9.2. Terminación

La ER debe informar 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. Los procedimientos necesarios serán establecidos por la Comisión de Reglamentos Técnicos y Comerciales del INDECOPI, en conformidad a la legislación vigente.

Documento de uso interno. Su contenido es confidencial y está destinado exclusivamente al personal autorizado de BIGDAVI S.A.C. Queda prohibida su reproducción, distribución o divulgación sin la autorización expresa de la Gerencia.

13.9.3. Efecto de terminación y supervivencia

La ER debe establecer en su RPS u otra documentación relevante las provisiones de divisibilidad, supervivencia y fusión, incluyendo las mismas en los contratos de suscriptor y tercero que confía.
Las ECs deberán establecer, en coordinación con la ER, en sus modelos de contratos de suscriptor y terceros que confían, cláusulas de supervivencia, de modo que ciertas reglas continúen vigentes después del término de validez de la CPS, RPS y de los contratos de los suscriptores y terceros que confían.

13.10. NOTIFICACIONES Y COMUICACIONES INDIVIDUALES CON LOS PARTICIPANTES

Las EC y ERs deben establecer, en sus contratos de suscriptor y terceros que confían, cláusulas de notificación que regulen los procedimientos por los que las partes se notifiquen hechos mutuamente.

13.11. Enmendaduras

13.11.1. Procedimiento para enmendaduras

INDECOPI revisará los cambios efectuados a las políticas y prácticas documentadas por la ER, antes que estos puedan implementarse. La documentación puede requerir una revisión.

13.11.2. Mecanismos y periodo de notificación

Los cambios en las políticas y prácticas de la ER deben ser notificados a los suscriptores, terceros que confían y otras partes tales como otras infraestructuras que reconocen al mismo o ECs con las que existen acuerdos de certificación cruzada, cuando dichos cambios puedan afectarles.
Cualquier cambio en los términos y condiciones básicas (identificadores de políticas, limitaciones de uso, obligaciones de suscriptor, forma de validación de un certificado, limitaciones a responsabilidad, procedimiento de resolución de disputas, periodo dentro del cual los registros de auditoría serán conservados, sistema legal aplicable y conformidad según el marco de la IOFE) deberá ser notificado a los suscriptores y terceros que confían.
Las ERs acreditadas, deben advertir a los suscriptores y potenciales terceros que confían la forma de notificación de esta información y las implicaciones de dicha notificación.

13.12. Provisiones sobre resolución de disputas

Se debe asegurar que los PSCs, ECs o ERs acreditados tengan establecido un procedimiento de resolución de disputas. Un prestador de servicios de certificación acreditado debe establecer procedimientos de resolución de disputas en su CP u otra documentación relevante. Se pueden establecer diferentes leyes aplicables para diferentes tipos de procesos de resolución de disputas.
De ser posible y permitido por las leyes correspondientes, debe considerarse el empleo de resolución de disputas en línea.

13.13. Ley aplicable

La ER debe identificar en su RPS y otra documentación relevante la ley aplicable a sus operaciones de acuerdo a la Ley N° 27269 y el Reglamento de Ley de Firmas y Certificados Digitales, aprobado por el D.S. 004-2007-PCM.
Los requerimientos legalmente significativos deben de estar establecidos o referenciados en los contratos de suscriptores y terceros que confían.

13.14. Conformidad con la ley aplicable

La ER debe identificar en su CP y otra documentación, las leyes aplicables a sus operaciones. Los requerimientos legales significativos deben estar establecidos o referenciados en los contratos de suscriptor y tercero que confía.

Documento de uso interno. Su contenido es confidencial y está destinado exclusivamente al personal autorizado de BIGDAVI S.A.C. Queda prohibida su reproducción, distribución o divulgación sin la autorización expresa de la Gerencia.

13.15. Cláusulas misceláneas

La ER debe incluir en su RPS y otra documentación toda cláusula miscelánea que se aplique a las operaciones que realiza bajo la IOFE.
De ser apropiado, estas provisiones deben ser establecidas o referenciadas en los contratos de suscriptores o terceros que confían.

13.15.1. Acuerdo íntegro

La ER debe establecer en sus contratos de suscriptor y tercero que confía cualquier otra documentación que pueda ser incorporada al mismo.

La EC en convenio con la ER, debe establecer en sus contratos de suscriptor y terceros que confían, cláusulas de acuerdo íntegro. En virtud de la cual se entenderá que el instrumento jurídico regulador del servicio contiene la voluntad completa y todos los acuerdos entre las partes.

13.15.2. Subrogación

Los derechos y los deberes asociados a la condición de ER no podrán ser objeto de cesión a terceros de ningún tipo, ni ninguna tercera entidad podrá subrogarse en la posición jurídica de dichas entidades.
La ER debe establecer en su documentación cualquier limitación en la subrogación de derechos o delegación de obligaciones.
Cuando un contrato de suscriptor cubre a múltiples titulares, toda limitación en la subrogación de derechos o delegación de obligaciones a dichos titulares, debe de estar establecida en el acuerdo.

13.15.3. Ejecución (tarifas de abogados y cláusulas de derechos)

La ER debe establecer en su RPS y otra documentación relevante toda cláusula de ejecución que se aplique a las operaciones que realiza. Estas cláusulas deben estar establecidas o referenciadas en los contratos de suscriptor y tercero que confía.

13.15.4. Fuerza mayor

Las ECs vinculadas en convenio con la ER, deben asegurar que las cláusulas de “fuerza mayor” sean establecidas explícitamente en los contratos de suscriptor y tercero que confía.

13.15.5. Otras cláusulas

La ER debe incluir en su RPS y otra documentación relevante cualquier otra cláusula que se aplique a las operaciones que realiza bajo la IOFE. Cuando fuere apropiado, estas cláusulas deben estar establecidas o referenciadas en los contratos de los suscriptores o terceros que confían.

14. Control de cambios

Versión	Fecha	Descripción de la modificación	Responsable
1.0	10/11/2021	Versión inicial	Dueño de proceso
2.0	15/10/2026	Se actualiza el diseño de la hoja de presentación conforme a la nueva imagen corporativa de la	Dueño de proceso

Documento de uso interno. Su contenido es confidencial y está destinado exclusivamente al personal autorizado de BIGDAVI S.A.C. Queda prohibida su reproducción, distribución o divulgación sin la autorización expresa de la Gerencia.

	empresa, incorporando el nuevo logotipo.	

Documento de uso interno. Su contenido es confidencial y está destinado exclusivamente al personal autorizado de BIGDAVI S.A.C. Queda prohibida su reproducción, distribución o divulgación sin la autorización expresa de la Gerencia.