DECLARACIÓN DE PRÁCTICAS DE SERVICIO DE VALOR AÑADIDO FIRMA REMOTA

Versión 1.1

INDICE

CONTROL DE VERSIONES

N° de versión	Fecha de actualización	Descripción del cambio
1.0	06/01/2026	Versión inicial.
1.1	12/01/2026	En el numeral 2.1.3 Obligaciones del suscriptor/titular, Se incorpora un punto adicional que establece la obligación del suscriptor de cerrar su sesión al finalizar el uso del servicio.

1. INTRODUCCIÓN

1.1. Alcance

El presente documento define, de manera “muy acotada”, el alcance, los límites y las prácticas mínimas del Servicio de Valor Añadido (SVA) de “Firma Remota” ofrecido por BIGDAVI S.A.C. (en adelante, “BIGDAVI”) a sus clientes (suscriptores/titulares), en coordinación con un tercero proveedor de infraestructura de firma remota: Camerfirma Perú (en adelante, “Camerfirma”).

El alcance del servicio comprende exclusivamente:

- Registro del solicitante y verificación de identidad por BIGDAVI en calidad de Entidad de Registro (ER), incluyendo la recopilación, validación y conservación de evidencias del proceso de identificación conforme a normativa aplicable y a las guías de acreditación vigentes.
- Gestión de la solicitud de emisión del certificado y su canalización segura hacia Camerfirma, para que el par de claves sea generado dentro del HSM del proveedor (no exportable) y se emita el certificado correspondiente, bajo las políticas y procedimientos de Camerfirma.
- Provisión del servicio de firma remota a nivel de integración, operación comercial, soporte funcional y atención de incidentes de primer nivel por BIGDAVI.
- Ejecución de las operaciones criptográficas de firma remota y custodia de claves privadas dentro de la infraestructura de Camerfirma (HSM/SAM y componentes asociados), bajo control exclusivo del firmante mediante mecanismos de autenticación fuerte previos a cada operación de firma.
- Trazabilidad operativa mínima del servicio (solicitudes, altas, bajas, incidencias y comunicaciones), incluyendo los mecanismos de escalamiento entre BIGDAVI y Camerfirma.

Este documento NO reemplaza la Política de Certificación (CP), la Declaración de Prácticas de Certificación (CPS) ni las políticas de firma remota del proveedor Camerfirma. Tampoco describe en detalle la arquitectura interna del HSM/SAM ni los procedimientos internos de operación de Camerfirma; dichos aspectos se rigen por la documentación oficial del proveedor y por los acuerdos contractuales vigentes. BIGDAVI no custodia claves privadas de firmantes y no opera módulos criptográficos de firma remota.

1.2. Política de Firma Remota reconocida

BIGDAVI reconoce y adopta, en lo que resulte aplicable al servicio, la(s) Declaración(es) de Prácticas (CPS) y la(s) Política(s) de Certificación/Servicio de firma remota publicadas por Camerfirma. Estas políticas deben ser las vigentes y aprobadas por la Autoridad Administrativa Competente que corresponda, cuando aplique.

1.3. Comunidad y ámbito de aplicación

Este documento puede ser utilizado por suscriptores del servicio de firma remota de BIGDAVI y por terceros que confían, como base para comprender las prácticas declaradas y los límites de responsabilidad asociados.

1.3.1. Prestador del SVA - Firma Remota

BIGDAVI actúa como Prestador del SVA a nivel local (contratación, soporte y gestión comercial). La operación de la plataforma de firma remota y de los HSM utilizados para custodia de claves corresponde al tercero Camerfirma, conforme a sus políticas y contratos.

1.3.2. Servicios de Valor Añadido (SVA)

Servicios compuestos por tecnología y sistemas de gestión que utilizan certificados digitales garantizando autenticidad e integridad durante su aplicación.

1.3.3. Política de Servicios de Valor Añadido (PSVA)

Conjunto de reglas que indican el marco de aplicabilidad del servicio para una comunidad de usuarios definida.

1.3.4. Suscriptor / Titular

Persona natural o jurídica que contrata el servicio a BIGDAVI y autoriza el uso de su certificado (emitido por la CA correspondiente) para la realización de firmas remotas. El suscriptor/titular acepta los términos y condiciones contractuales, así como las obligaciones descritas en este documento.

1.3.5. Tercero que confía (Relying Party)

Persona o entidad que recibe un documento o transacción firmada remotamente y decide confiar en la validez de la firma y del certificado asociado, previa validación técnica y legal correspondiente.

1.3.6. Declaración de Prácticas de Servicio de Valor Añadido (DPSVA)

Procedimientos y controles adoptados en cada etapa del servicio y sistemas brindados a los clientes, de acuerdo con lo establecido por INDECOPI (y demás normativa aplicable).

1.3.7. Ámbito de aplicación y usos

El SVA “Firma Remota” permite a los suscriptores generar firmas digitales/electrónicas sobre documentos o transacciones electrónicas mediante el uso de un certificado digital cuyas claves privadas permanecen

bajo custodia en HSM, y cuya activación requiere autorización del titular mediante mecanismos de autenticación fuerte (p.ej., segundo factor).

- Firma de documentos electrónicos (ej. PDF PAdES u otros formatos soportados por la plataforma).
- Firma de transacciones en sistemas corporativos (workflows, portales, sistemas documentales).
- Uso con sellado de tiempo cuando el flujo/cliente lo requiera (servicio adicional o integrado).

1.3.8. Usos prohibidos y no autorizados

No se permite el uso del servicio para fines contrarios a la normativa peruana, o para finalidades distintas de las autorizadas por el contrato, la política reconocida y la aplicabilidad del certificado. Queda prohibido, entre otros:

- El uso fraudulento o suplantación de identidad.
- El uso del servicio sin autorización expresa del titular, o el uso compartido de credenciales/factores de autenticación.
- El uso del servicio para actividades ilícitas o que vulneren derechos de terceros.
- La alteración, intento de extracción o uso no autorizado de material criptográfico.

1.3.9. Conformidad y contacto

Esta DPSVA es administrada por BIGDAVI S.A.C. y constituye el marco público de prácticas del SVA “Firma Remota”. Para consultas, incidentes o solicitudes formales, utilice los siguientes canales (a completar según corresponda):

- **Responsable:** Wilfredo Dávila Fuentes
- **Cargo:** Gerente General
- **E-mail:** wilfredo.davila@bigdavi.com
- **Teléfono:** +(51) 979 661 983 / 500 5160 / 359 6616
- **Dirección:** Pj. Mártir Olaya 129 Of. 1905, Miraflores, Lima - Perú (si aplica).

La Gerencia General de BIGDAVI S.A.C., constituye la autoridad de la presente Declaración de Prácticas y velará por su cumplimiento de los lineamientos técnicos y legales que le sean de aplicación, así como las buenas prácticas, estableciendo las medidas y controles que considere necesario a tal efecto.

2. OBLIGACIONES Y RESPONSABILIDADES

2.1. Obligaciones

2.1.1. Obligaciones del proveedor del SVA - Firma Remota (BIGDAVI)

BIGDAVI asume, como mínimo, las siguientes obligaciones frente a suscriptores y terceros que confían, sin perjuicio de lo establecido en el contrato y en las políticas reconocidas:

- Gestionar la contratación, provisión comercial y soporte de primer nivel del servicio.
- Actuar como Entidad de Registro (ER) en los procesos de verificación de identidad para la emisión del certificado asociado a la firma remota, cuando aplique.
- Custodiar y tratar la información del suscriptor conforme a la Ley N° 29733 (Protección de Datos Personales) y a los acuerdos contractuales.
- Registrar y conservar evidencias operativas mínimas (ej. trazas de solicitud, autorización y entrega del servicio) según normativa/contrato.
- Escalar a Camerfirma los incidentes o requerimientos que correspondan a la plataforma y HSM de terceros.

2.1.2. Obligaciones del tercero proveedor de infraestructura (Camerfirma)

La infraestructura de firma remota, incluyendo la generación/custodia de claves en HSM y la plataforma de firma, es responsabilidad de Camerfirma. En consecuencia, Camerfirma debe cumplir, como mínimo, con los siguientes requisitos auditables (sin perjuicio de su CP/CPS vigente):

1. La clave privada del suscriptor será generada en el módulo criptográfico del dispositivo criptográfico del prestador del servicio (HSM del proveedor). El mismo requerimiento es aplicable para el proceso de creación de las firmas remotas: la operación criptográfica se ejecuta dentro del HSM.
2. La generación de claves debe realizarse exclusivamente con datos de exclusivo conocimiento y control del suscriptor.
3. El sistema debe estar configurado de modo que impida que el prestador del servicio pueda conocer las claves privadas de los suscriptores, ya sea por acceso directo, registro de operaciones (logs), gestión administrativa o cualquier vulnerabilidad de su arquitectura (no-exportabilidad, segregación de funciones y control dual cuando aplique).
4. El dispositivo criptográfico de creación de claves del prestador del servicio debe ser independiente del dispositivo criptográfico de la Entidad de Certificación que emitió el certificado digital asociado a la

firma remota (por ejemplo, segregación entre HSM de CA y HSM de firma remota).

5. El prestador del servicio debe contar con un sitio principal y uno de contingencia para garantizar continuidad. El sitio de contingencia también contará con su dispositivo criptográfico de creación de firmas remotas. La verificación de condiciones idóneas se llevará a cabo mediante visitas presenciales, salvo que se cuente con certificaciones de cumplimiento aplicables según normativa vigente.
6. Se requerirá el cumplimiento de las siguientes especificaciones:
    - El dispositivo de firma (HSM) deberá contar con una certificación de cumplimiento del estándar CEN-EN 419.221, parte 5 ("Módulo Criptográfico para Servicios de Confianza") u otro equivalente.
    - Antes de autorizar la firma, el sistema exigirá al usuario autenticarse mediante mecanismos de factor múltiple: OTP (One Time Password), biometría u otros de nivel equivalente.
    - El sistema debe registrar evidencias de la transacción de firma, auditables y provistas de sello de tiempo, y garantizar técnicamente que el firmante tenga control exclusivo sobre el acto de firma en los términos descritos por la normativa aplicable (incluyendo D.S. 052-2008-PCM y modificatorias).
    - Respecto a la integridad de los datos que se firmarán, el sistema debe mostrarlos al usuario de forma clara e inequívoca antes de la firma. En ningún momento el sistema permitirá una manipulación de dicha visualización. Además, contará con mecanismos o componentes que permitan verificar la autenticidad de la firma generada.
    - El sistema demostrará resistencia a ataques de replay, phishing y “intermediario u hombre en el medio” (MITM), y utilizará canales seguros como TLS y cifrado de extremo a extremo cuando aplique.

2.1.3. Obligaciones del suscriptor/titular

El suscriptor/titular se obliga a:

- Proveer información veraz y completa durante la verificación de identidad y solicitud de emisión del certificado.
- Mantener bajo control exclusivo sus factores de autenticación (contraseñas, OTP, dispositivo móvil, etc.) y no compartirlos.
- Revisar y aceptar la aplicabilidad del certificado y las condiciones del servicio antes de su uso.
- Notificar de inmediato a BIGDAVI cualquier sospecha de compromiso, pérdida o uso no autorizado de credenciales, y solicitar revocación cuando corresponda.
- Usar el servicio únicamente para los fines permitidos por el contrato y la política reconocida.

- El suscriptor debe cerrar su sesión al finalizar el uso del servicio y evitar dejarla abierta en equipos compartidos o entornos donde terceros puedan acceder sin autorización. El descuido en esta práctica constituye un uso negligente y puede comprometer la seguridad de su certificado.

2.1.4. Obligaciones de los terceros que confían

Los terceros que confían deben:

- Validar la firma y el certificado asociado antes de confiar (integridad, cadena de confianza, vigencia, revocación, sellado de tiempo si aplica).
- Verificar la aplicabilidad del certificado (uso permitido) y cualquier limitación de responsabilidad declarada en las políticas vigentes.
- No depender del servicio para finalidades o niveles de garantía no contratados/establecidos en la política reconocida.

2.2. Responsabilidad

2.2.1. Exoneración de responsabilidad

Sin perjuicio de lo que establezcan los contratos y la normativa aplicable, BIGDAVI no será responsable por pérdidas derivadas de: (i) uso indebido o fraudulento del servicio; (ii) incumplimiento de obligaciones del suscriptor; (iii) fraude o falsedad en la información proporcionada por el solicitante; (iv) eventos de fuerza mayor; y (v) fallas atribuibles a terceros fuera del control razonable de BIGDAVI, incluyendo componentes y operación de infraestructura provistos por Camerfirma.

2.2.2. Límite de responsabilidad

Los límites de responsabilidad financiera (reembolsos, indemnizaciones, extensiones de garantías) serán los definidos contractualmente para cada cliente/servicio.

3. PUBLICACIÓN DE LA DECLARACIÓN DE PRÁCTICAS

La DPSVA del SVA - Firma Remota de BIGDAVI, así como documentación relevante (políticas, privacidad, condiciones) será publicada en el portal institucional de BIGDAVI o el que se designe para tal fin en la siguiente dirección: https://bigdavi.com/peru/acreditaciones/, el documento debe publicarse firmado por el responsable del SVA y con control de versiones.

4. CONTROLES DE SEGURIDAD FÍSICA, INSTALACIONES, GESTIÓN Y OPERACIONALES

4.1. Cumplimiento

El SVA - Firma Remota estará sujeto a auditorías y revisiones periódicas, conforme a la normativa y a los acuerdos con proveedores y clientes.

4.2. Evaluación de riesgo

BIGDAVI y/o sus proveedores realizan análisis de riesgo de seguridad de la información que incluyen identificación de amenazas, evaluación de impacto y planes de mitigación.

4.3. Control de acceso a los ambientes

Los ambientes utilizados para prestar el servicio deben contar con acceso restringido y controles de seguridad física. En el caso de infraestructura en centros de datos de terceros (Camerfirma o su data center), aplican los controles declarados en sus políticas y contratos.

4.4. Control de acceso y acceso a usuarios

Se aplican controles de acceso lógico por roles (mínimo privilegio), autenticación robusta y trazabilidad. Para actividades críticas relacionadas con material criptográfico, se exige segregación de funciones y, cuando aplique, control dual en el proveedor de infraestructura.

4.5. Autorización para retirar equipos o sistemas fuera del local

Cualquier retiro de equipos o medios con información asociada al servicio se rige por procedimientos formales y autorización expresa, conforme a políticas internas y de proveedores.

4.6. Gestión de activos

Los activos de BIGDAVI vinculados al servicio (plataformas de integración, portales, sistemas de soporte) se mantienen inventariados y bajo control.

4.7. Seguridad de recursos humanos

El personal con acceso a información o sistemas críticos debe pasar verificaciones de antecedentes y recibir capacitación acorde a su rol.

4.8. Gestión de incidentes

El servicio cuenta con dos niveles de atención de incidentes: primer nivel por BIGDAVI (mesa de ayuda/tickets) y segundo nivel por Camerfirma para incidentes que requieran

intervención en la plataforma y HSM. Se mantiene registro y trazabilidad de incidentes y su resolución.

4.9. Seguridad de la información - antivirus / software malicioso

Los sistemas servidores de BIGDAVI y/o sus proveedores cuentan con mecanismos de protección contra software malicioso (antivirus, EDR u otros) y procedimientos de actualización.

5. POLÍTICA DE REEMBOLSO

Las condiciones de reembolso serán definidas en los respectivos contratos con cada cliente, de acuerdo con el tipo de servicio y alcance contratado.

6. RESPONSABILIDAD FINANCIERA, REPRESENTACIONES Y GARANTÍAS

La cobertura de seguro, provisiones de garantía y responsabilidad e indemnizaciones se definen contractualmente con cada cliente, de acuerdo con el tipo de servicio y cliente.

7. ENMENDADURAS

Los procedimientos para resolución de enmendaduras y correcciones se definen contractualmente con cada cliente, de acuerdo con el tipo de servicio y cliente.

8. RESOLUCIÓN DE DISPUTAS

Los procedimientos para resolución de disputas se definen contractualmente con cada cliente, de acuerdo con el tipo de servicio y cliente.

9. ACUERDO ÍNTEGRO, SUBROGACIÓN Y DIVISIBILIDAD

Las cláusulas de acuerdo íntegro, subrogación y divisibilidad se definen contractualmente con cada cliente, de acuerdo con el tipo de servicio y cliente.

10. FUERZA MAYOR Y OTRAS PROVISIONES

Las cláusulas de fuerza mayor y otras provisiones aplicables se definen contractualmente con cada cliente, de acuerdo con el tipo de servicio y cliente.

11. TARIFAS

Las tarifas por los servicios serán definidas en los contratos con los clientes y en las cotizaciones emitidas por BIGDAVI.

12. COBERTURA DEL SEGURO

La cobertura del seguro (si aplica) será la definida contractualmente con cada cliente y/o la que mantenga el proveedor de infraestructura según sus políticas.

13. FINALIZACIÓN DEL SVA

En caso de cese del servicio, BIGDAVI comunicará a sus clientes con la anticipación establecida contractualmente y adoptará medidas para asegurar continuidad de verificación y trazabilidad dentro de los límites regulatorios y contractuales, coordinando con Camerfirma cuando corresponda.

14. CONFORMIDAD CON LA LEY APLICABLE

Este documento se emite bajo la normativa peruana aplicable a la Infraestructura Oficial de Firma Electrónica (IOFE), lineamientos y guías de acreditación del INDECOPI, así como las obligaciones contractuales de BIGDAVI. Como referencia de buenas prácticas, se consideran estándares internacionales aplicables a servicios de firma remota (p.ej., ETSI para servicios de confianza y políticas de firma remota).

15. BIBLIOGRAFÍA

- INDECOPI: Guías de acreditación y Marco de Política de Prestación de Servicios de Valor Añadido (Anexo 1).
- RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.