2026

Política de Certificación v2.0

1 INFORMACIÓN DEL DOCUMENTO

1.1. NOMBRE Y RESPONSABLE

Nombre del documento	Política de Certificación de BPO
Responsable documento	Representante Legal
Tipo de documento	Público
Realizado por	Responsable de Cumplimiento
Código	BPO IOFE PL2 V 2.0

1.2 CONTROL DE VERSIONES

Versión	Fecha de vigencia	Aprobación	Comentario
1.0	A la aprobación del Indecopi	Representante legal de Perú	Creación del documento

1.3 OID

OID	1.3.6.1.4.1.50718.0.1.0.1.1

2. INTRODUCCIÓN

BPO ADVISORS SPA, SUCURSAL DEL PERÚ ("BPO") presta servicios relacionados con la identificación digital, la firma electrónica avanzada y cualificada, integrables en plataformas web a nivel global.

BPO está acreditado en Perú como **Entidad de Certificación Digital (EC)**, **Autoridad de Sellado de Tiempo (TSA)** y **Prestador de Servicios de Valor Añadido del tipo FIRMA REMOTA**.

BPO presta servicios de emisión, revocación y re-emisión de certificados digitales, siguiendo la regulación de la Infraestructura Oficial de Firma Electrónica (IOFE).

---

3. OBJETIVO

El objetivo de este documento es describir las operaciones y prácticas que utiliza BPO para la administración de sus servicios como Entidad de Certificación Digital (EC), en el marco del cumplimiento de los requerimientos de la "Guía de Acreditación de Entidades de Certificación Digital (EC)" establecida por el INDECOPI.

---

4. OBJETO DE LA ACREDITACIÓN

El alcance de la acreditación cubre la infraestructura y procesos de los servicios de certificación digital brindados por la Entidad de Certificación BPO.

---

5. DEFINICIONES Y ABREVIACIONES

Definiciones Clave:

- **Entidad de Certificación (EC):** Entidad que presta servicios de emisión, revocación, re-emisión, modificación, suspensión de certificados digitales en el marco de la regulación establecida por la IOFE.
- **Autoridad de Sellado de Tiempo (TSA):** Entidad que emite sellos de tiempo.
- **Titular:** Persona natural o jurídica a cuyo nombre se expide un certificado digital y que actúa como responsable del mismo.
- **Suscriptor:** Persona natural responsable del uso de la clave privada, a quien se le vincula de manera exclusiva con un documento electrónico firmado digitalmente.

- **Módulo Criptográfico (QSCD):** Un Módulo Criptográfico de Hardware (HSM) que almacena las claves privadas bajo el control exclusivo del suscriptor y opera en modo Common Criteria (CC) QSCD según el **CEN-EN 419 221-5**.

5.3. PARTICIPANTES

- **ENTIDAD DE CERTIFICACIÓN BPO (EC BPO):** Persona jurídica privada que presta servicios inherentes a la certificación digital y es responsable de los trámites ante la AAC para ingresar a la IOFE.
- **ENTIDAD DE REGISTRO BPO:** Entidad afiliada a BPO que valida la información del solicitante, verifica su identidad y realiza su registro.
- **SISTEMA DE FIRMA REMOTA:** Modalidad de Prestador de Servicios de Valor Añadido que permite operaciones de creación de firma digital usando claves privadas localizadas remotamente y gestionadas por un tercero (BPO).

---

6. SERVICIOS DE CERTIFICACIÓN DIGITAL

BPO brinda los servicios de emisión, re-emisión, revocación y distribución de los certificados digitales.

---

7. RESPONSABILIDADES

BPO garantiza las responsabilidades contractuales, garantías financieras y coberturas de seguros requeridas. La Entidad de Registro afiliada brinda los servicios de registro y verificación de identidad conforme a las Guías de Acreditación del INDECOPI.

---

8. USO DEL CERTIFICADO

8.1. TIPOS DE CERTIFICADOS

BPO emite, entre otros, los siguientes tipos de certificados:

1. **Certificado de Persona Natural:** Para que una persona natural se acredite y firme digitalmente. Incluye certificados custodiados por el suscriptor (en un token o repositorio software certificado como FIPS 140-2).
2. **Certificado cuya clave privada será custodiada en el servicio de Firma Remota (Clave Custodiada):** Certificado cuya clave privada es **generada, custodiada y gestionada por BPO** como Prestador de Servicios de Valor Añadido de Firma Remota. La clave se almacena en un **Módulo Criptográfico de Hardware (HSM)**

certificado como QSCD (EN 419 221-5), bajo la premisa de **Control Exclusivo** del firmante. Su uso requiere la **autorización explícita y multifactor** del suscriptor.

3. **Certificado de Persona Jurídica:** Identifica al firmante como Representante legal o Apoderado o empleado de una Organización.
4. **Certificado de Agente Automatizado:** Identifica a un dispositivo informático de una persona jurídica que realiza operaciones automáticas de firma o descifrado.

8.2. USOS ADECUADOS DEL CERTIFICADO

- **Identificación del Titular:** El Titular puede autenticar su identidad.
- **Integridad del documento firmado:** Garantiza que el documento no fue alterado después de la firma.
- **No repudio de origen:** Garantiza que el Titular que ha firmado no puede negar la autoría o la integridad del documento.

8.3. USOS PROHIBIDOS DEL CERTIFICADO Se prohíbe el uso cuando contravengan la Ley de Firmas y Certificados Digitales – Ley 27269, las Guías de Acreditación del INDECOPI o sus anexos.

---

9. PERSONA DE CONTACTO

La persona de contacto para consultas relacionadas con la Política y Declaración de Prácticas de Certificación de BPO es Teresa Prado Alarcón (Teléfono: +56 951104076, Correo electrónico: teresa.prado@bpo-advisors.net, Página Web: https://idok.pe/).

---

10. RESPONSABILIDADES DE LOS TITULARES Y SUSCRIPTORES

Es responsabilidad del suscriptor: conservar y dar uso adecuado al certificado; resguardar su clave privada; proteger el uso de su certificado mediante PIN; informar a BPO inmediatamente cualquier situación que afecte la validez del certificado o si su clave privada se ve comprometida; y realizar un uso adecuado según el contrato. En el caso del servicio de Firma Remota, el Suscriptor debe **autenticarse mediante mecanismos de factor múltiple (MFA)** para generar el Dato de Activación de Firma (SAD) y autorizar explícitamente y activar la clave privada (SCD) para la operación de firma.

---

11. GESTIÓN DEL CICLO DE VIDA DE LAS CLAVES

11.1. GENERACIÓN DE LAS CLAVES

- **Claves de la EC:** Generadas en un entorno asegurado físicamente, bajo control dual y en un dispositivo que cumple con FIPS 140-2 nivel 3.

- **Claves del Suscriptor (Firma Remota):** Generadas directamente **dentro de un Módulo Criptográfico Hardware (HSM) certificado y configurado conforme al Estándar CEN 419 221 - 5**. Estas claves se generan mediante el **RNG interno** del HSM y se asocian con el **atributo de autorización de firma** para garantizar el Control Exclusivo del suscriptor.
- **Tamaño Mínimo:** La longitud de la clave RSA para firmar certificados (emisor) y para el suscriptor (entidad final) es de **2048 bits** (con un máximo de 3 años de uso para el suscriptor).

11.2. PROTECCIÓN DE LA CLAVE PRIVADA

- **EC:** La clave privada se mantiene y usa en un dispositivo criptográfico seguro, cumpliendo los requerimientos **FIPS 140-2 nivel 3**. Se realiza copia de respaldo, almacenada en forma cifrada y bajo control dual.
- **Firmante (Firma Remota):** La clave privada permanece protegida por las claves criptográficas del **Módulo Criptográfico certificado CEN 419 221-5** durante todo su ciclo de vida. **No existe duplicidad o archivo** de estas claves. La clave se configura con el atributo que exige la autorización de firma por parte del suscriptor (Control Exclusivo).

11.5. TÉRMINO DEL CICLO DE VIDA DE LA CLAVE PRIVADA Si el certificado de clave pública es revocado, la clave privada correspondiente debe ser **destruida**.

---

12. CICLO DE VIDA DEL MÓDULO CRIPTOGRÁFICO

12.1. GESTIÓN DEL CICLO DE VIDA DEL MÓDULO CRIPTOGRÁFICO El HSM utilizado (para EC y Firma Remota) está certificado y configurado conforme al **Estándar CEN 419 221-5**. Se aplican procedimientos de seguridad que incluyen protección del módulo durante el transporte (sellado) y su borrado (zeroización) antes de ser retirado.

---

13. AUTENTICACIÓN

No aplica; los certificados no se utilizan para la autenticación en el control de acceso a la plataforma.

---

14. CIFRADO

No aplica; los certificados no se utilizan para el cifrado de la información como funcionalidad de la plataforma.

---

15. CANALES SSL

15.3. VALIDACIÓN DEL ESTADO DE REVOCACIÓN BPO realiza un monitoreo y control continuo de la vigencia de los certificados. Cuando un certificado SSL es revocado, el navegador consulta la Lista de Revocación de Certificados (CRL) y bloquea el acceso.

---

16. CONSULTA DE SELLOS DE TIEMPO

16.1. FORMATO DE PETICIÓN El formato de petición de sellos de tiempo es conforme a la **RFC 3161**.

16.2. VALIDACIÓN DE CONFIABILIDAD DE LA RAÍZ Se utiliza el certificado de TSU de BPO, emitido por la Autoridad de Sellado de Tiempo acreditada por el INDECOPI.

---

17. GESTIÓN DE LA SEGURIDAD

17.1. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN El equipo de gestión de seguridad incluye un **Chief Information Security Officer** y un **Responsable de Cumplimiento**.

17.5. SEGURIDAD FÍSICA Y DEL ENTORNO La Política de Seguridad Física de BPO establece directivas para la protección de zonas seguras y **centros de datos proveedores**, incluyendo control de ingreso físico y monitoreo. El Centro de Datos Principal de BPO (GTD Panamericana) cuenta con certificaciones **TIER III**.

17.10. SEGURIDAD EN REDES Se requiere y filtra la conexión de sistemas (mediante **firewalls**), se detecta y autentica la conexión de equipos, y se segregan los canales de administración de red. La información que se transfiere por redes no seguras se realiza de forma **cifrada mediante protocolos SSL**.

---

18. TÉRMINO DE LA ORGANIZACIÓN QUE ADMINISTRA EL SVA

18.1. PREPARACIÓN ANTES DEL TÉRMINO En caso de cese de la actividad de la EC, se informará al INDECOPI, a los suscriptores y terceros que confían con al menos **treinta (30) días calendario de anticipación**. BPO proveerá los fondos necesarios (mediante seguro de responsabilidad civil) para continuar las actividades de revocación y mantendrá los certificados activos y el sistema de verificación/revocación hasta su extinción.

---

19. REGISTROS DE AUDITORÍA

19.1. EVENTOS REGISTRADOS Se registran eventos relacionados con las transacciones de autenticación y generación de firma digital. Los eventos significativos incluyen las solicitudes o transacciones de firma digital.

19.2. PROTECCIÓN DE LOS REGISTROS Los registros de auditoría se protegen contra la manipulación para asegurar su integridad. El periodo de retención es de al menos **10 años**.

---

20. AUDITORÍA

20.4. AUDITOR Los evaluadores para los procesos de acreditación deben ser autorizados por la AAC y ser **independientes del PSVA**, sin haber realizado trabajos para este dentro de los 2 años anteriores a la auditoría.

---

21. CONFORMIDAD CON LA LEY APLICABLE

BPO se adhiere y cumple con las obligaciones establecidas por la IOFE, la Guía de Acreditación de Prestador de Servicios de Valor Añadido SVA, el Reglamento de la Ley de Certificados Digitales y la Ley de Firmas y Certificados Digitales – Ley 27269.