BPO ADVISORS | iDOK

2026

Declaración de Prácticas de Servicios de Valor Añadido tipo SID - FIRMAYA



Índice

1 INFORMACIÓN DEL DOCUMENTO 5
1.1. NOMBRE Y RESPONSABLE 5
1.2 CONTROL DE VERSIONES 5
2 INTRODUCCIÓN 6
3 OBJETIVO 6
4 OBJETO DE LA ACREDITACIÓN 6
5 DEFINICIONES Y ABREVIACIONES 6
5.1 ABREVIACIONES 6
5.2 DEFINICIONES 8
5.3 PKI PARTICIPANTES 8
5.3.1 ENTIDAD DE CERTIFICACIÓN BPO (EC BPO) 8
5.3.2 ENTIDAD DE REGISTRO BPO 8
5.3.3 AUTORIDAD DE SELLADO DE TIEMPO (TSA BPO) 9
5.3.4 SISTEMA DE INTERMEDIACIÓN DIGITAL 9
5.3.5 SISTEMA DE FIRMA REMOTA 9
5.3.6 SUSCRIPTOR DEL SID 9
5.3.7 FIRMANTE 9
5.3.7 TERCERO QUE CONFÍA 9
6 REQUERIMIENTOS SOBRE LAS PRÁCTICAS DEL SID 10
6.1 ORGANIZACIÓN QUE ADMINISTRA LOS DOCUMENTOS 10
6.2 PERSONA DE CONTACTO 10
7 FRECUENCIA DE PUBLICACIÓN 11
8 PUBLICACIÓN Y DIFUSIÓN DEL DOCUMENTO 11
9 SISTEMA DE INTERMEDIACIÓN DIGITAL COMO SERVICIO 11
10 RESPONSABILIDADES Y OBLIGACIONES DEL PSVA 12
14 EXONERACIÓN DE RESPONSABILIDAD 13
15 Gestión del ciclo de vida de las claves 14
15.1 Generación de las claves 14
15.2 Protección de la clave privada 14
15.3 Distribución de la clave pública 15
15.4 Re-emisión de la clave 15
15.5 Término del ciclo de vida de la clave privada 15
16 Ciclo de vida del módulo criptográfico. 15
16.1 Gestión del ciclo de vida del módulo criptográfico 15
17 Autenticación 15
No aplica, no se utilizan los certificados para la autenticación en el control de acceso a la plataforma. 15
18 Cifrado 15
No aplica, no se utilizan los certificados para el cifrado de la información como funcionalidad de la plataforma. 15
19 Canales SSL 15
19.1 Protección de la clave privada 15

19.2 Validación de la confiabilidad de la raíz 16
19.3 Validación del estado de revocación 16
19.4 Validación del estado de vigencia 16
19.5 Validación del propósito 16
20 Consulta de sellos de tiempo 16
20.1 Formato de petición 16
20.2 Validación de confiabilidad de la raíz 16
20.3 Validación del estado de revocación 17
20.4 Validación del estado de vigencia 17
20.5 Validación de la firma 17
21 Gestión de la seguridad 17
21.1 Organización de la seguridad de la información 17
21.2 Política de seguridad de la información 17
21.3 Seguridad en el trato con terceros 17
21.4 Seguridad del personal 18
21.5 Seguridad física y del entorno 18
21.6 Gestión de operaciones 18
21.7 Manejo de medios y seguridad 18
21.8 Planificación del sistema 19
21.9 Reporte y respuesta a incidentes 19
21.10 Seguridad en redes 19
21.11 Monitoreo 20
21.12 Intercambio de datos y software 20
21.13 Gestión de accesos a los sistemas 20
21.14 Archivo 20
21.15 Desarrollo y mantenimiento de sistemas confiables 21
21.16 Control de cambios 21
22 Término de la organización que administra el SVA 21
22.1 Preparación antes del término 21
23 Registros de auditoría 21
23.1 Eventos registrados 21
23.2 Protección de los registros 22
23.3 Eventos significativos 22
24 Auditoría 22
24.1 Auditoría de registros 22
24.2 Auditoría del archivo 22
24.3 Auditoría de los procedimientos y controles 22
24.4 Auditor 22
25.1 Políticas de reembolso 22
25.2 Cobertura de seguro de responsabilidad civil 23
25.3 Información confidencial y/o privada 23
25.4 Información no privada 23

25.5 Derechos de propiedad intelectual 24
25.6 Notificaciones y comunicaciones entre participantes 24
25.7 Procedimiento de resolución de disputas 24
25.8 Conformidad con la ley aplicable 25
25.9 Exención de garantías 25
25.10 Indemnizaciones 25
25.11 Fuerza mayor 25
26 CONFORMIDAD CON LA LEY APLICABLE 26
27 BIBLIOGRAFÍA 26

1 INFORMACIÓN DEL DOCUMENTO

1.1. NOMBRE Y RESPONSABLE

Nombre del documento	Declaración de Servicios de Valor Añadido tipo SID de BPO, FIrmaYa con firma remota y tokens
Responsable del documento	Representante Legal
Tipo de documento	Público
Realizado por	INNOVATE DC

1.2 CONTROL DE VERSIONES

Versión	Fecha de vigencia	Aprobación	Comentario
1.0	08 Noviembre 2025	CTO	Creación del documento

2 INTRODUCCIÓN

BPO ADVISORS SPA, SUCURSAL DEL PERÚ, en adelante "BPO", es una empresa fundada en 2016 que provee servicios relacionados con la identificación digital, firma electrónica avanzada y cualificada (firma digital), integrables en sistemas documentales y plataformas web a nivel global. BPO se enfoca en la autenticación de identidad, la garantía de la manifestación de voluntad en procesos digitales y la eliminación de la suplantación de identidad en transacciones con valor legal. En este contexto, BPO incursiona como Entidad de Certificación, Autoridad de Sellado

de Tiempo, Entidad de Registro, Sistema de Intermediación Digital, Servicio de Firma Remota y Software de Firma Digital.

El presente documento se centra en describir las funcionalidades y la operación de "FirmaYa", el Sistema de Intermediación Digital (SID) de BPO. FirmaYa facilita la transmisión y el almacenamiento seguro de información, garantizando el no repudio, la confidencialidad y la integridad de las transacciones mediante componentes de firma digital, autenticación y canales seguros. Asimismo, se detallan las prácticas y procedimientos que BPO implementa para la administración de sus servicios como SID, en cumplimiento de los requisitos establecidos por la "Guía de Acreditación de Prestador de Servicios de Valor Añadido SVA", modalidad SID del INDECOPI.

3 OBJETIVO

Este documento tiene como objetivo la descripción de las operaciones y prácticas que utiliza BPO para la administración de sus servicios como Sistema de Intermediación Digital, en el marco del cumplimiento de los requerimientos de la "Guía de Acreditación de Prestador de Servicios de Valor Añadido SVA", modalidad SID establecida por el INDECOPI.

4 OBJETO DE LA ACREDITACIÓN

El alcance de la acreditación cubre la infraestructura y procesos de los servicios de valor añadido tipo SID brindados por BPO como Prestadores de Servicios de Valor Añadido como Sistema de Intermediación Digital de BPO.

5 DEFINICIONES Y ABREVIACIONES

5.1 ABREVIACIONES

AAC	Autoridad Administrativa Competente
DN	Distinctive Name: Nombre Distintivo
EC	Entidad de Certificación
CPS	Certification Practice Statement: Declaración de Prácticas de Certificación
CRL	Lista de Certificados Revocados
IOFE	Infraestructura Oficial de Firma Electrónica

PC	Política de Certificación
RUC	Registro Único de Contribuyentes
SHA	Secure Hash Algorithm (Algoritmo de seguridad HASH)
CA	Certification Authority (Autoridad de Certificación)
DSCF	Dispositivo seguro de creación de firma
FIPS	Federal Information Processing Standards (Estándares Federales Procesamiento de la Información)
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
PKCS	Public-Key Cryptography Standards.
PKI	Infraestructura de llave pública
PSC	Prestador de Servicios de Certificación
RA	Autoridad de Registro
RFC	Request For Comments
RSA	Rivest, Shamir and Adleman.
SSL	Secure Sockets Layer
TSA	Time Stamping Authority
TSU	Time Stamping Unit

5.2 DEFINICIONES

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.

Entidad de Registro – ER	Entidad que realiza los procesos de verificación de identidad de los solicitantes de los servicios de certificación digital y que custodia de forma segura las evidencias de dichos procesos.
Autoridad de Sellado de Tiempo -TSA	Entidad que emite los sellos de tiempo.
Declaración de Prácticas de Certificación	Es el documento en el que consta de manera detallada los procedimientos que aplica la EC para la prestación de sus servicios. Una declaración de las prácticas que una EC emplea para emitir, gestionar, revocar y renovar certificados sin y con cambio de claves.
Política de Certificación	Conjunto de reglas que indican el marco de aplicabilidad de los servicios para una comunidad de usuarios definida.
Titular	Entidad que requiere los servicios provistos por la EC de BPO, y que está de acuerdo con los términos y condiciones de los servicios conforme a lo declarado en el presente documento.
Tercero que confía	Persona que recibe un documento, log, o notificación firmado digitalmente, y que confía en la validez de las transacciones realizadas.

5.3 PKI PARTICIPANTES

5.3.1 ENTIDAD DE CERTIFICACIÓN BPO (EC BPO)

BPO, en su papel de Entidad de Certificación, es la persona jurídica privada que presta indistintamente servicios de producción, emisión, gestión, revocación, cancelación u otros servicios inherentes a la certificación digital.

BPO, como Entidad de Certificación, le corresponderá la realización de todos los trámites y procedimientos ante la AAC a fin de poder ingresar a la IOFE.

5.3.2 ENTIDAD DE REGISTRO BPO

BPO, a través de su Entidad de Registro de BPO o alguna ER afiliada a la EC de BPO, será la encargada de validar la información suministrada por el solicitante de un certificado digital, mediante la verificación de su identidad y su registro.

5.3.3 AUTORIDAD DE SELLADO DE TIEMPO (TSA BPO)

BPO brinda también los servicios de Autoridad de Sellado de Tiempo, la cual se encarga de emitir sellos de tiempo. Un sello de tiempo es un conjunto de datos que representa el resumen de un documento sellado añadido a un registro del tiempo en el que el sello fue emitido. Este resumen es una característica única del documento, de modo que si el documento es modificado este sello pierde validez. Las particularidades sobre el uso, y especificaciones de la TSA, se describen en la respectiva Política de Sellado de Tiempo de BPO.

5.3.4 SISTEMA DE INTERMEDIACIÓN DIGITAL

FirmaYa, como servicio de BPO, actúa como un sistema de intermediación digital que facilita la transmisión y el almacenamiento seguro de información. Este servicio garantiza el no repudio, la confidencialidad y la integridad de las transacciones a través del uso de componentes de firma digital, autenticación y canales seguros.

En este contexto, FirmaYa optimiza la gestión documental, de identificación y de firma electrónica y digital, permitiendo a empresas y personas firmar documentos de manera segura y con plena validez legal, simplificando sus procesos y ofreciendo soluciones para la firma masiva de documentos.

5.3.5 SISTEMA DE FIRMA REMOTA

BPO brinda también servicios de firma remota como una modalidad de Prestador de Servicios de Valor Añadido que permite efectuar operaciones de creación de firma digital utilizando claves privadas que se encuentran localizadas remotamente y son gestionadas por un tercero.

5.3.6 SUSCRIPTOR DEL SID

El Suscriptor o cliente es la persona que se suscribe al servicio de FirmaYa, en calidad de sistema de intermediación digital, para realizar firmas o enviar invitaciones de firma a terceros.

5.3.7 FIRMANTE

Aquel que realiza el proceso de firma, ya sea porque es suscriptor de la plataforma FirmaYa, o porque recibe una invitación para firmar de parte de un suscriptor.

5.3.8 TERCERO QUE CONFÍA

Tercero que confía son todas aquellas personas naturales o jurídicas que deciden aceptar y confiar en los documentos firmados a través del servicio de FirmaYa en calidad de sistema de intermediación digital. El Tercero que confía, puede ser o no titular.

5.3.9 MÓDULO DE ACTIVACION INFORMATICA

El SAM es un componente de software configurado cuya función principal es garantizar, con un alto nivel de confianza, que las claves de firma se utilizan bajo el control exclusivo (sole control) del firmante dentro del sistema de firma remota.

5.3.10 CABFORUM

CA/Browser Forum (o CAB Forum) es un consorcio voluntario formado por autoridades de certificación (CA) y proveedores de navegadores web (como Google, Microsoft, Mozilla) que establece estándares y "requisitos básicos" (Baseline Requirements) para la emisión y gestión de certificados digitales SSL/TLS y de firma de código, garantizando la seguridad en las transacciones de Internet.

6 REQUERIMIENTOS SOBRE LAS PRÁCTICAS DEL SID

6.1 ORGANIZACIÓN QUE ADMINISTRA LOS DOCUMENTOS

BPO administra los documentos Política y Declaración de Prácticas del Servicios de Valor Añadido, Política y Plan de Seguridad, Política y Plan de Privacidad, y todos los documentos normativos del SID de BPO.

Para cualquier consulta contactar:

Correo electrónico:	contacto@idok.pe
Página Web:	https://idok.pe/

6.2 PERSONA DE CONTACTO

Para consultas en general puede comunicarse por vía telefónica, correo electrónico o acercándose directamente a las oficinas de BPO.

Correo electrónico:	contacto@idok.pe
Página Web:	https://idok.pe/

7 FRECUENCIA DE PUBLICACIÓN

Con autorización del Responsable de la EC y el SID de BPO y el INDECOPI, se publicará la versión finalmente aprobada. Los cambios generados en cada nueva versión serán previamente informados al INDECOPI y publicados en la página web

de BPO junto con la nueva versión. La auditoría anual validará estos cambios y emitirá el informe de cumplimiento.

8 PUBLICACIÓN Y DIFUSIÓN DEL DOCUMENTO

El Responsable del SID de BPO es el encargado de la autorización de la publicación de la Política y Declaración de Prácticas SVA y es responsable de asegurar la integridad y disponibilidad de la información publicada en la página Web:

https://idok.pe/

9 SISTEMA DE INTERMEDIACIÓN DIGITAL COMO SERVICIO

9.1 DESCRIPCIÓN DEL SERVICIO:

FirmaYa, el servicio de BPO, actúa como un sistema de intermediación digital que facilita la transmisión de documentos para su firma digital. Este servicio garantiza el no repudio, la confidencialidad y la integridad de las transacciones a través del uso de componentes de firma digital, autenticación y canales seguros.

En este contexto, FirmaYa optimiza la gestión documental, de identificación y de firma electrónica y digital, permitiendo a empresas y personas firmar documentos de manera segura y con plena validez legal, simplificando sus procesos y ofreciendo soluciones para la firma masiva de documentos. Además, FirmaYa puede utilizar los sellos de tiempo de BPO para dar fecha y hora cierta en los actos de firma. Las claves privadas utilizadas en este sistema corresponden a los firmantes y son gestionadas por el sistema de firma remota de BPO, o bien por módulos criptográficos de software o hardware propios del firmante.

10 RESPONSABILIDADES Y OBLIGACIONES DEL PSVA

Las responsabilidades y obligaciones principales de BPO se centran en la prestación del servicio de firma digital con firma remota o tokens, garantizando una disponibilidad de la plataforma conforme a los SLA contratados. Además, BPO tiene la obligación de proteger la Información Confidencial del cliente, usándola únicamente para la ejecución del servicio contratado y tomando medidas razonables contra su divulgación.

11 RESPONSABILIDADES Y OBLIGACIONES DEL SUSCRIPTOR

El suscriptor tiene la responsabilidad de utilizar el servicio bajo las prácticas descritas en la Política y Declaración de Prácticas de Valor Añadido. Adicionalmente, el cliente está obligado a gestionar todas las comunicaciones por escrito a las direcciones especificadas y, al igual que BPO, debe proteger la

Información Confidencial recibida, utilizándola únicamente para los fines del contrato y dando aviso inmediato en caso de divulgación no autorizada.

12 RESPONSABILIDADES DE LOS FIRMANTES

Protección de la Clave Privada: Mantener la confidencialidad y la seguridad de la clave privada asociada al certificado. En el caso de la firma remota, deberá proteger la información de autenticación y autorización de firma.

Uso Adecuado: Utilizar el certificado digital únicamente para los propósitos establecidos en la Política y Declaración de Prácticas de Certificación.

Notificación de Compromiso: Solicitar inmediatamente la revocación del certificado si la clave privada ha sido comprometida o existe la sospecha de ello a la EC o ER correspondiente.

Información Precisa: Asegurarse de que toda la información proporcionada para la emisión del certificado es exacta y completa.

13 RESPONSABILIDADES DE LOS TERCEROS QUE CONFÍAN

Verificación del Estado del Certificado: Es fundamental que el Tercero que Confía verifique la validez y el estado de revocación del certificado utilizado en el documento firmado antes de aceptarlo y confiar en la firma o la identidad que representa.

Uso Consistente: El Tercero que Confía debe asegurarse de que el certificado con el que se firmó el documento se esté utilizando para los propósitos previstos y dentro de los límites de responsabilidad establecidos en la política.

Conocimiento de la Política: Asumir los riesgos asociados al uso del certificado con el que se firmó el documento, lo que implica conocer y aceptar los términos y condiciones definidos en la Política y Declaración de Prácticas de Certificación.

14 EXONERACIÓN DE RESPONSABILIDAD

El SID de BPO no será responsable de garantizar la operación en ningún caso cuando se encuentran ante cualquiera de estas circunstancias:

- Estado de Guerra, desastres naturales o cualquier otro caso de Fuerza Mayor
- Fuera de la aplicabilidad permitida en este documento.

- Uso indebido o fraudulento de los certificados digitales de BPO, y los servicios del SID.
- Incumplimiento de las obligaciones establecidas para el Suscriptor o Terceros que confían en la normativa vigente o en las prácticas descritas en el presente documento.
- Por el contenido de los mensajes o documentos firmados o cifrados digitalmente.
- Fraude en la documentación presentada por el solicitante.

15 Gestión del ciclo de vida de las claves

BPO es afecta y cumple con las obligaciones establecidas por la IOFE, los requerimientos de 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, para el reconocimiento legal de los servicios que brinda el SID de BPO bajo las directrices definidas en el presente documento.

En este marco, se destaca que las claves utilizadas por FirmaYa, que son custodiadas por BPO, corresponden a la clave privada de cada firmante operando a través de su servicio de firma remota, por lo que solamente pueden ser utilizadas bajo control exclusivo del firmante. Estas claves son custodiadas de forma segura desde su generación en un sistema centralizado, bajo el control exclusivo del suscriptor. Para garantizar la máxima seguridad y validez legal, cada acción de firma requiere la participación activa en la autenticación y autorización explícita del firmante.

15.1 Generación de las claves

En este marco, se destaca que las claves utilizadas por FirmaYa corresponden a la clave privada de cada firmante. Estas claves son generadas en un módulo criptográfico hardware (HSM) certificado y configurado conforme al Estándar CEN 419 221 - 5, y son custodiadas de forma segura en un sistema centralizado, bajo el control exclusivo del suscriptor de las claves, el posterior firmante. La clave privada de cada firmante es protegida de manera individual por el HSM.

15.2 Protección de la clave privada

Como parte del servicio de firma remota, la clave privada del suscriptor permanece durante todo su ciclo de vida dentro módulo criptográfico certificado y configurado conforme al Estándar CEN 419 221 - 5. En casos de contingencia puede ser exportado cifrado protegido por las claves criptográficas del HSM, para ser importado en un equipo HSM con la misma configuración. No existe duplicidad o archivo de las claves privadas.

15.3 Distribución de la clave pública

Una vez generado el par de claves en el módulo criptográfico, el servicio de firma remota se encargará de producir un CSR, que es un formato estándar para enviar la clave pública y otra información relevante a la CA.

15.4 Re-emisión de la clave

No se realiza una re-emisión de clave privada.

15.5 Término del ciclo de vida de la clave privada

Si el certificado de clave pública es revocado, la clave privada correspondiente debe ser destruida.

16 Ciclo de vida del módulo criptográfico.

16.1 Gestión del ciclo de vida del módulo criptográfico

El módulo criptográfico hardware (HSM) utilizado corresponde al que se usa para la protección de las claves privadas del firmante en el servicio de firma remota. Este módulo está certificado y configurado conforme al Estándar CEN 419 221 - 5, conforme a lo permitido en la Resolución 175-2025/DGI-INDECOPI.

17 Autenticación

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

18 Cifrado

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

19 Canales SSL

19.1 Protección de la clave privada

La clave privada se protege en el key store del servidor de aplicaciones.

19.2 Validación de la confiabilidad de la raíz

El certificado es emitido por una Entidad de Certificación de Confianza que se encuentra dentro de [1]CABFORUM.

19.3 Validación del estado de revocación

Cuando un certificado SSL es revocado, el navegador muestra una advertencia de seguridad al usuario porque ya no puede verificar la identidad del sitio, bloqueando el acceso o indicando que la conexión no es segura. Esto ocurre porque el navegador consulta la Lista de Revocación de Certificados (CRL) de la Autoridad de Certificación (CA) que emitió el certificado y lo encuentra en la lista de certificados inválidos, impidiendo la conexión segura. BPO realiza un monitoreo y control continuo de la vigencia de los certificados.

19.4 Validación del estado de vigencia

Cuando un certificado SSL expira, el navegador marca el sitio como inseguro, mostrando advertencias, eliminando el candado de seguridad y, en algunos casos, bloqueando el acceso. BPO realiza un monitoreo y control continuo de la vigencia de los certificados.

19.5 Validación del propósito

El navegador valida el propósito de la clave del certificado SSL a través de la extensión "Uso de la clave". Los navegadores verifican si el propósito de la clave (por ejemplo, cifrado, firmas, etc.) es apropiado para la operación que se intenta realizar, y rechazan certificados que no cumplen con estas restricciones para garantizar una conexión segura.

20 Consulta de sellos de tiempo

20.1 Formato de petición

El formato de petición es conforme a la RFC 3161.

---

[1] CA/Browser Forum (o CAB Forum) es un consorcio voluntario formado por autoridades de certificación (CA) y proveedores de navegadores web (como Google, Microsoft, Mozilla) que establece estándares y "requisitos básicos" (Baseline Requirements) para la emisión y gestión de certificados digitales SSL/TLS y de firma de código, garantizando la seguridad en las transacciones de Internet

20.2 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.

20.3 Validación del estado de revocación

Si un certificado de TSU es revocado, es retirado del sistema y la clave privada es eliminada, por lo que no se utilizará para emitir sellos de tiempo.

20.4 Validación del estado de vigencia

Si un certificado de TSU expira, es retirado del sistema y la clave privada es eliminada, por lo que no se utilizará para emitir sellos de tiempo.

20.5 Validación de la firma

La firma correcta del sello de tiempo se puede verificar al usar un validador.

21 Gestión de la seguridad

21.1 Organización de la seguridad de la información

BPO cuenta con un equipo organizado para gestionar el Sistema de Seguridad de la Información:

- Chief Information Security Officer (Director de Seguridad de la Información): Encargado de la ciberseguridad y seguridad de la información.
- Responsable de Cumplimiento: Responsable de velar por el cumplimiento normativo técnico PKI, ciberseguridad y protección de datos personales.
- Operaciones: Responsables de la gestión de infraestructura y monitoreo de seguridad.

21.2 Política de seguridad de la información

La dirección del SGSI de BPO se compromete a proteger la confidencialidad, integridad, disponibilidad y autenticidad de la información, y a gestionar la seguridad mediante un modelo de mejora continua.

21.3 Seguridad en el trato con terceros

BPO cuenta con una política para la gestión de proveedores, la cual establece un marco integral para la seguridad en la gestión de proveedores de BPO, con el objetivo de proteger los sistemas de información de la empresa. Incluyendo la preparación, la selección de proveedores, la contratación detallando obligaciones contractuales clave, como la clasificación de la información, requisitos legales, gestión de incidentes y auditorías. Durante el onboarding, se gestiona la transferencia segura de información, se otorgan accesos controlados y se evalúan

los riesgos. La implementación se enfoca en estrategias de contingencia, pruebas de seguridad y el monitoreo de componentes de la cadena de suministro.

21.4 Seguridad del personal

La Política de seguridad en la gestión de recursos humanos de BPO tiene como objetivo establecer directivas generales para la gestión de la seguridad de la información, abarcando desde el proceso de selección, con verificaciones de antecedentes y competencias, hasta los términos y condiciones de empleo que incluyen acuerdos de confidencialidad y responsabilidades legales. También se enfoca en la concientización, educación y capacitación periódica del personal sobre seguridad de la información, un proceso disciplinario graduado para infracciones, y la gestión de responsabilidades de seguridad tras la terminación o cambio de empleo.

21.5 Seguridad física y del entorno

La Política de Seguridad Física de BPO tiene como objetivo establecer directivas para la protección y gestión de entornos de zonas seguras y centros de datos proveedores, salvaguardando la confidencialidad, integridad y disponibilidad de los recursos y datos. Esta política, relevante para el personal, proveedores y terceros interesados, abarca perímetros de seguridad física, control de ingreso físico con mecanismos de autenticación, aseguramiento de oficinas y salas, monitoreo por sistemas de vigilancia, y protección contra amenazas físicas y ambientales. También incluye medidas para el trabajo en áreas seguras, ubicación y protección de equipos, seguridad de activos fuera de las instalaciones, gestión de medios de almacenamiento, servicios de suministro, mantenimiento de equipos, eliminación segura de equipos e información, gestión de capacidad, redundancia de instalaciones de procesamiento de información, logueo y monitoreo de actividades.

21.6 Gestión de operaciones

La Política de Seguridad de la Infraestructura de BPO tiene como objetivo establecer directivas generales para las medidas de seguridad en el control de accesos dentro del alcance del SGSI. Las etapas clave incluyen la seguridad en el uso de servicios en la nube, la gestión de capacidad y configuración, el enmascaramiento de datos, el respaldo de información, el logueo, el monitoreo de actividades, la sincronización de relojes, el uso de programas de utilidad privilegiados, la instalación de software en sistemas operacionales, la seguridad y segregación de redes, el uso de criptografía, la protección de sistemas durante pruebas y la eliminación de información.

21.7 Manejo de medios y seguridad

La Política de Gestión de Activos de BPO tiene como objetivo establecer directivas generales para la identificación, registro y mantenimiento continuo de todos los activos de información y recursos relevantes dentro de la organización. Es fundamental para salvaguardar la integridad y disponibilidad de los recursos, basándose en la identificación, clasificación y protección efectiva de los activos. Las etapas clave incluyen el inventario actualizado de activos tangibles e intangibles, la clasificación de activos según su valor, relevancia y sensibilidad (confidencialidad, integridad, disponibilidad), la asignación clara de roles y responsabilidades, la implementación de medidas de protección y control, y la auditoría y monitoreo continuo para detectar anomalías y asegurar la efectividad de los controles. Todos los activos dentro del alcance del SGSI son protegidos y gestionados durante todo su ciclo de vida.

21.8 Planificación del sistema

La Política de Desarrollo Seguro de BPO tiene como objetivo establecer directivas generales y máximas en la gestión de la seguridad de la información. La seguridad en el desarrollo de software implica la aplicación de requisitos de seguridad en cada etapa del ciclo de vida del software, desde la concepción hasta la implementación y el mantenimiento, garantizando la protección de la información y la confianza de los usuarios. El documento aborda aspectos clave como la planificación (consideraciones legales y contractuales, separación y seguridad de entornos, y seguridad en las actividades del proyecto), el desarrollo subcontratado, la gestión de la seguridad en la cadena de suministro de TIC, el diseño (requisitos de diseño, protección de datos, arquitectura segura, autenticación y procedimientos de inicio de sesión), la codificación segura, las pruebas (revisión de código, escaneo de vulnerabilidades y pruebas de penetración), la puesta en producción, la operación y la gestión de cambios de desarrollo.

21.9 Reporte y respuesta a incidentes

La Política de Gestión de Incidentes de Seguridad de BPO contempla la planificación y preparación, incluyendo la definición de roles, comunicación de eventos, categorización y priorización de incidentes, registro de resultados, monitoreo, detección, clasificación, análisis y reporte. También establece procedimientos para la respuesta a incidentes, asignación de responsabilidades, manejo de evidencia digital, escalada, registro de actividades, comunicación con partes interesadas, cierre formal de incidentes, análisis forense y post-incidente, e identificación de vulnerabilidades.

21.10 Seguridad en redes

La Política de Seguridad de la Infraestructura de BPO aborda la gestión de redes estableciendo responsabilidades y procedimientos para la administración de

equipos y dispositivos de red. Esto incluye mantener la documentación actualizada, como diagramas de red y archivos de configuración, y separar las responsabilidades operativas de las redes de las operaciones del sistema cuando sea apropiado. Se restringe y filtra la conexión de sistemas a la red (por ejemplo, mediante firewalls), se detecta, restringe y autentica la conexión de equipos y dispositivos, y se segregan los canales de administración de red de otro tráfico. Además, se deshabilitan los protocolos de red vulnerables y se identifican e implementan medidas de seguridad necesarias para servicios de red específicos, como autenticación y cifrado.

21.11 Monitoreo

En BPO, el sistema de monitoreo abarca el tráfico de red, sistema y aplicación (tanto entrante como saliente), los registros de eventos relacionados con la actividad del sistema y de la red, y el uso de recursos como CPU, discos duros, memoria y ancho de banda, así como su rendimiento. Hemos definido una línea base de comportamiento normal y monitoreamos activamente las anomalías en comparación con esta base. Utilizamos software de monitoreo automatizado, configurado para generar alertas basadas en umbrales predefinidos. Además, las configuraciones de hardware, software, servicios y redes se monitorean continuamente con herramientas de administración del sistema y se revisan periódicamente para verificar los ajustes, evaluar la seguridad de las contraseñas y las actividades realizadas.

21.12 Intercambio de datos y software

La Política de Transferencia de Información de BPO cubre la información en tránsito, especificando que la información confidencial sólo debe transferirse por medios cifrados y por personal autorizado, sin generar copias no autorizadas y registrando todas las transacciones.

21.13 Gestión de accesos a los sistemas

La Política de Control de Accesos de BPO segrega las funciones de control de acceso en solicitud, autorización y administración, y requiere que los propietarios de la información asignen restricciones de acceso según los requisitos de seguridad y clasificación de activos. También aborda la gestión de identidades, la información de autenticación, los derechos de acceso (incluyendo autorización formal y procedimientos de provisión y revocación), la restricción de accesos para evitar fugas de información sensible o anónima, el acceso al código fuente, la autenticación segura (con múltiples factores para sistemas críticos), la prevención de fuga de datos mediante identificación y monitoreo, y la gestión de derechos de acceso privilegiado a través de un proceso de autorización.

21.14 Archivo

En BPO, se realiza el respaldo en servicios de nube adecuados que garantizan la recuperación de toda la información y el software esenciales después de cualquier incidente, falla o pérdida de medios de almacenamiento. Hemos desarrollado e implementado planes detallados sobre cómo la organización respalda la información, software y sistemas, abordando nuestra política específica sobre copias de seguridad.

21.15 Desarrollo y mantenimiento de sistemas confiables

En BPO, se utilizan principios de codificación segura tanto para nuevos desarrollos como para escenarios de reutilización. Estos principios se aplican a las actividades de desarrollo dentro de la organización y para los productos y servicios que proporcionamos a otros. Se emplean técnicas de programación seguras como programación en pares, refactorización, revisión por pares, iteraciones de seguridad y desarrollo basado en pruebas. Respecto a herramientas y bibliotecas externas, se cuenta con la licencia, seguridad e historial de los componentes externos.

21.16 Control de cambios

El procedimiento de gestión de cambios de desarrollo regula la creación o modificación de software, y la actualización de parches. Las solicitudes se registran y planifican, identificando propósitos, riesgos, recursos y responsabilidades.

22 Término de la organización que administra el SVA

22.1 Preparación antes del término

Se realizará la comunicación a través de una publicación en la página web de BPO y una notificación de correo electrónico. La página web del BPO (https://idok.pe/) será el canal principal para la publicación de esta información.

Se evaluarán todas las obligaciones contractuales pendientes con los clientes, incluyendo servicios de soporte, garantía o cualquier otro servicio comprometido y realizar el tratamiento correspondiente.

23 Registros de auditoría

23.1 Eventos registrados

Se registran eventos relacionados con las transacciones de autenticación y generación de firma digital.

23.2 Protección de los registros

Los eventos son registrados de manera que no puedan ser borrados o destruidos dentro del periodo requerido como evidencia, a menos que sean transferidos a medios de almacenamiento de largo plazo.

23.3 Eventos significativos

Se registran las solicitudes o transacciones de firma digital.

24 Auditoría

24.1 Auditoría de registros

Los registros son evaluados durante los periodos de auditoría. Tanto durante las auditorías de seguridad como las auditorías de acreditación por parte del INDECOPI en calidad de Autoridad Administrativa Competente, cada año.

24.2 Auditoría del archivo

El archivo es evaluado durante los periodos de auditoría. Tanto durante las auditorías de seguridad como las auditorías de acreditación por parte del INDECOPI en calidad de Autoridad Administrativa Competente, cada año.

24.3 Auditoría de los procedimientos y controles

Los procedimientos y controles implementados son auditados por la Autoridad Administrativa Competente, cada año.

24.4 Auditor

Los evaluadores para los procesos de acreditación deben cumplir los siguientes requisitos:

- Ser autorizado por la AAC.
- Ser independiente del PSVA y no haber realizado trabajos para este dentro de los 12 meses anteriores a la ejecución de la auditoría.

25 Aspectos legales de la operación del PSC

25.1 Políticas de reembolso

BPO no contempla la realización de reembolsos, salvo que se especifique lo contrario en el contrato con el cliente.

25.2 Cobertura de seguro de responsabilidad civil

La cobertura de seguro de responsabilidad civil de BPO se extiende a todos los servicios que ofrece como PSC, conforme a los montos estipulados por la IOFE.

25.3 Información confidencial y/o privada

Se considera como "Información Confidencial" a una amplia gama de información de ambas partes, que incluye:

- Investigación, desarrollo, secretos comerciales, procesos, fórmulas, planes de negocios, estrategias, presupuestos, relaciones con clientes y distribuidores, e información financiera y comercial.
- Información técnica, know-how, hardware, software, diseños, políticas de seguridad, claves de acceso, configuraciones de filtración e información de integridad o seguridad de la red o sistemas de computación del cliente.
- Los métodos, sistemas, datos y materiales utilizados o proporcionados por BPO para ofrecer los servicios.

Obligaciones estipuladas en el contrato:

- Ambas partes (Clientes y BPO) se comprometen a usar la información Confidencial únicamente en relación con el cumplimiento de las obligaciones estipuladas en su contrato.
- Cada parte (Clientes y BPO) se compromete a tomar medidas razonables (no menos estrictas que las empleadas para proteger su propia información) para evitar su divulgación a terceros.
- Se prohíbe usar o revelar la información a otra persona sin el previo consentimiento por escrito de la otra parte, a menos que sea requerido por ley. En este último caso, la parte requerida debe notificar a la otra para que tenga la oportunidad de objetar o tomar medidas para preservar el carácter confidencial.

25.4 Información no privada

No se considera "Información Confidencial" aquella información que:

- Ha sido conocida por la parte receptora antes de su revelación.
- Se encuentre públicamente disponible sin una acción u omisión de la parte receptora.
- Ha sido recibida legalmente de un tercero.
- Está constituida por información estadística u otra sobre vulnerabilidad o configuraciones, siempre que no identifique al cliente, su red o sistemas de computación.

25.5 Derechos de propiedad intelectual

Contractualmente, el cliente y BPO realizan los siguientes acuerdos:

- No Adquisición de Derechos: El cliente y BPO se comprometen recíprocamente a no adquirir derecho, título o interés alguno sobre la información, datos, herramientas, procesos o metodologías que sean propiedad de la otra parte.
- Propiedad Intelectual y Activos Intangibles: Esta disposición abarca, pero no se limita a, los derechos de autor, marcas registradas, marcas de servicio, secretos comerciales, patentes y cualquier otra forma de propiedad intelectual o activo intangible de la otra parte.
- Uso de Marcas Comerciales: Ninguna de las partes utilizará las marcas registradas, marcas de servicio, nombres comerciales o nombres de productos de la otra parte, salvo que dicho uso esté expresamente autorizado mediante licencia específica otorgada conforme al Contrato y sus Anexos.

25.6 Notificaciones y comunicaciones entre participantes

- Formato de los Avisos: Todo aviso que una parte deba dar a la otra debe efectuarse por escrito.
- Medios de Comunicación Aceptados:
  - Carta certificada.
  - Entrega personal a las direcciones indicadas.
  - Correos electrónicos.
- Validez: Los avisos solo serán válidos si se remiten a las direcciones postales o de correos electrónicos indicadas a continuación, a menos que alguna de las partes haya notificado a la otra una nueva dirección.

Correo electrónico:	contacto@idok.pe
Página Web:	https://idok.pe/

25.7 Procedimiento de resolución de disputas

Las peticiones, quejas o reclamos presentados por suscriptores y terceros de los servicios del Sistema de Intermediación Digital (SID) deben ser dirigidas a BPO para su atención y resolución directa a través de los siguientes canales de contacto:

Tipo	Canal
Ticket de reclamo	contacto@idok.pe

Sin perjuicio de la atención directa por parte de BPO, los suscriptores y terceros que confían tienen el derecho de presentar su reclamo, según corresponda, ante el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI), de acuerdo con lo dispuesto en el Código de Protección y Defensa del Consumidor (Ley N° 29571) y su normativa complementaria.

25.8 Conformidad con la ley aplicable

BPO se adhiere y cumple con las obligaciones establecidas por:

- La Infraestructura Oficial de Firma Electrónica (IOFE).
- Los requerimientos de la Guía de Acreditación de Prestador de Servicios de Valor Añadido SVA.
- El Reglamento de la Ley de Certificados Digitales.
- La Ley de Firmas y Certificados Digitales – Ley 27269.

Este cumplimiento asegura el reconocimiento legal de los servicios brindados por el SID de BPO bajo las directrices definidas en el documento.

25.9 Exención de garantías

Inexistencia de Otras Garantías: Todos los servicios e ítems susceptibles de entrega proporcionados por BPO se proporcionan “tal como están”, exceptuando las declaraciones y garantías mutuas contenidas en sus respectivos contratos.

25.10 Indemnizaciones

En caso de incumplimiento, el cliente podrá ejercer las acciones de reclamación y aplicar las penalizaciones conforme a lo especificado en sus contratos.

25.11 Fuerza mayor

Ninguna de las partes será considerada en mora o responsable de otro modo por el incumplimiento de sus obligaciones cuando se deba a causas fuera de su control, incluyendo:

- Eventos Específicos: Incendio, inundación, tormenta de nieve substancial, epidemia, accidente, explosión, siniestro, huelga, paro provocado por la empresa, controversia laboral, tumulto, perturbación civil, acción del enemigo, embargo, guerra.
- Actos de Autoridad: Una ordenanza o ley municipal, o una orden ejecutiva, administrativa o judicial (siempre que no sea resultado de un incumplimiento previo).
- Fallas Técnicas Mayores: Cualquier falla o demora de un sistema de transporte, energía, computación o comunicaciones, u otra causa similar fuera del control de la parte.

26 CONFORMIDAD CON LA LEY APLICABLE

BPO se adhiere y cumple con las obligaciones establecidas por:

- La Infraestructura Oficial de Firma Electrónica (IOFE).
- Los requerimientos de la Guía de Acreditación de Prestador de Servicios de Valor Añadido SVA.
- El Reglamento de la Ley de Certificados Digitales.
- La Ley de Firmas y Certificados Digitales – Ley 27269.

Este cumplimiento asegura el reconocimiento legal de los servicios brindados por el SID de BPO bajo las directrices definidas en el documento.

27 BIBLIOGRAFÍA

a) Política y Declaración de Prácticas de Certificación de BPO
b) Guía de Acreditación de Prestador de Servicios de Valor Añadido SVA, INDECOPI
c) Ley de Firmas y Certificados Digitales – Ley 27269
d) Reglamento de la ley de Firmas y Certificados Digitales, aprobado mediante el Decreto Supremo Nro. 052-2008 y sus modificatorias
e) Resolución N° 175-2025/DGI-INDECOPI