ANEXO I:

MARCO DE LA POLÍTICA DE PRESTACIÓN DE SERVICIOS DE VALOR AÑADIDO

1. Declaración e implementación de las Prácticas

Los Prestadores de servicios de Valor Añadido deben elaborar y establecer como documento normativo su respectiva Declaración de Prácticas –DPSVA, mediante el cual la entidad deberá declarar los procedimientos y controles que adopta en cada etapa de los servicios y sistemas que brinda a sus clientes. El documento Política de Servicios de Valor Añadido también puede ser definido respecto de las prácticas y especificaciones de los servicios específicos de valor añadido. Sin embargo, este documento puede ir contenido en la DPSVA o disgregado según los diferentes productos a variaciones de SVA que en PSVA puede tener.

Los controles establecidos en el documento DPSVA y/o la Política de Sellado de Tiempo y su contenido, deben estar de acuerdo con lo establecido por la Autoridad Administrativa Competente, en el presente documento. Las evaluaciones realizadas por la Autoridad Administrativa Competente velarán porque los controles implementados por la entidad que solicita la acreditación sean conformes a los requerimientos expresados en el presente documento y a lo declarado por la entidad en su respectiva DPSVA.

En las siguientes secciones se describen los requerimientos que deben ser implementados en los procedimientos y operación de los Prestadores de Servicios de Valor Añadido, según el tipo de servicio que brindan, y que deben ser declarados en su documento DPSVA.

Gestión del documento			
Explicación preliminar: Puesto que el documento Declaración de Prácticas de Valor Añadido es un documento normativo, que implica una obligación frente a los clientes del SVA, este documento debe ser adecuadamente gestionado a fin de mantener su autenticidad, vigencia, actualización y publicación.			
No	Requerimiento		Detalle
1	Nombre e identificación del documento	El documento de declaración deberá tener un código identificador, el cual deberá ser	

		colocado de manera visible en la carátula del documento	
2	Control de versiones	El documento deberá mostrar en la carátula, el control de versiones respectivo.	
3	Organización que administra los documentos del SVA	Se debe indicar el nombre o razón social de la entidad o empresa que administra y es autora bajo responsabilidad ante el proceso de acreditación de la AAC, de la elaboración de los documentos normativos del SVA.	
4	Persona de contacto	Indicar los datos de contacto o canal de comunicación por el cual los terceros que confían y los titulares y los suscriptores de los certificados puedan referir sus consultas.	
5	Frecuencia de publicación	El SVA deberá indicar la frecuencia con la cual es actualizado y publicado el documento. La vigencia máxima de un documento DPSVA es de 1 año desde el logro de su acreditación, luego este reconocimiento debe ser validado anualmente por las revisiones de supervisión que realiza la AAC. En caso de actualizaciones mayores estas deben ser presentadas a la AAC antes de	

		realizar la modificación del documento. Una actualización mayor es aquella que afecta a los procesos de registro o verificación de identidad.	
6	Publicación y difusión del documento	El PSVA debe publicar su DPSVA al entrar en operación con el logro de la acreditación, a través de un medio público que permita su constante consulta por parte de titulares, suscriptores y terceros que confían.	

Alcance de aplicación del documento			
Explicación preliminar: El campo de usuarios que pueden ser afectos a los servicios del PSVA debe ser definido.			
No	Requerimiento		Detalle
7	Participantes	El PSVA deberá definir el campo de participantes o usuarios de los servicios que brinda, describiendo los tipos de titulares y terceros que son afectos al presente documento.	Por ejemplo: Pueden definirse limitaciones espaciales, profesionales, etc., como limitar el campo de usuarios a ciudadanos peruanos, al departamento de lima, o a un grupo profesional específico como los asociados al colegio de ingenieros, o los

			exportadores afiliados a la VUCE, etc.
8	Aplicabilidad	El PSVA deberá definir, si existen, los límites el campo de aplicabilidad o uso de los servicios que brinda.	
9	Conformidad	El PSVA debe ser evaluado periódicamente para evidenciar que sus operaciones y controles son conformes con los documentos normativos como la DSPVA o la Política de Servicios de Valor Añadido.	

2. AUTORIDAD DE SELLADO DE TIEMPO

Las Autoridades de Sellado de Tiempo son un tipo de SVA cuyos servicios permiten validar la fecha y hora cierta en el que se realiza una transacción electrónica. La confiabilidad de los servicios de la TSA se basa en la seguridad, integridad y confiabilidad de la clave privada con la que se firman los sellos de tiempo y la exactitud de la fecha y hora en función de la sincronización con una fuente de tiempo confiable. El marco de evaluación de los controles definidos para la Autoridad de Sellado de Tiempo está basado en la RFC 3628: Policy Requirements for Time-Stamping Authorities (TSAs), cuya equivalencia funcional en la Communidad Europea se define en el estándar ETSI 102 023

Las TSA deben ser evaluadas respecto del cumplimiento de los requerimientos descritos en la sección 8 y anexo I del presente documento. El cumplimiento del anexo I puede ser sustentado mediante una sesión de auditoría mediante la evaluación de los controles, registros y documentos normativos o mediante los informes de auditoría independiente, emitida por un agente autorizado o reconocido internacionalmente, que cubran los siguientes alcances:

- RFC 3628 o
- ETSI 102 023 o

- Webtrust for Certificate Authority + ISO 27001, siempre que las certificaciones en conjunto incluyan en su alcance la evaluación de las fuentes de tiempo confiable y la protección de la clave de firma de la TSA.
- Webtrust for Certificate Authority o ETSI 101 456, siempre que la certificación incluya en su alcance la evaluación de las fuentes de tiempo confiable y la protección de la clave de firma de la TSA y los controles de seguridad de la infraestructura de la TSA.

2.1. Definición de Responsabilidades

Responsabilidades			
Explicación preliminar: Se deben definir las responsabilidades de las partes.			
No	Requerimiento		Detalle
10	Política de Sellado de Tiempo	La TSA debe implementar un documento normativo conforme a los requerimientos descritos en la sección 8 y anexo I del presente documento.	En otros países se desarrolla la Política de Sellado de Tiempo en lugar de la DPSVA. El PSVA puede presentar la Política de sellado de tiempo, o la de Prácticas de Valor Añadido (DPSVA), o ambas. Lo que se debe asegurar es que se cubran todos los temas exigidos a la Autoridad de Sellado de Tiempo.
11	Responsabilidades y obligaciones de la TSA	La TSA deberá definir sus responsabilidades en relación con los usuarios de los sellos de tiempo y los terceros que confían.	
12	Responsabilidades y obligaciones del suscriptor	La TSA deberá definir las responsabilidades de los suscriptores, usuarios de los sellos de tiempo.	• Documento donde se establece la estructura de la TSA, especificando las subcontrataciones o tercerizaciones existentes y especificando sus

			responsabilidades y obligaciones • Documento donde se establecen los términos y condiciones de uso de los servicios de sellado de tiempo
13	Responsabilidades de los Terceros que confían	La TSA deberá definir las responsabilidades de los terceros que confían, incluyendo: • Verificar que el sello de tiempo ha sido correctamente firmado, y que la clave privada utilizada para firmar el sello de tiempo no debe haber sido comprometida hasta el momento de la verificación. • Tomar en cuenta cualquier limitación en el uso de los sellos de tiempo considerados en la Política de Sellado de Tiempo o en la DPSVA • Tomar en cuenta cualquier otra precaución prescrita en los acuerdos u otra parte.	Documento donde se establece el análisis de riesgo y la planificación correspondiente

14	Limitaciones de Responsabilidad	La TSA puede declarar o limitar cualquier responsabilidad excepto aquellas que sean estipuladas en las Regulación vigente.	
15	Resolución de disputas	El PSVA debe definir donde el cliente puede ser informado sobre los procedimientos para la resolución de disputas con sus clientes, indicando los datos de contacto o dirección a donde pueden dirigirse los reclamos, Estos procedimientos pueden ser establecidos en los contratos de prestación de los servicios con los clientes del PSVA o publicados en los documentos del PSVA	

2.2. Gestión del ciclo de vida de las claves

Gestión del ciclo de vida de las claves		
Explicación preliminar: El PSVA debe proteger la clave privada que emplea para firmar los sellos de tiempo a fin de evitar su compromiso.		
No	Requerimiento	Detalle

16	Generación de las claves de la TSA	a) La Generación de las claves de firma de la Unidad de Sello de tiempo deberá ser realizada en un ambiente asegurado físicamente, por personal que ocupa roles de confianza, bajo al menos el control de acceso de dos personas. El personal autorizado para realizar estas funciones debe estar limitado para realizar esta tarea conforme a los procedimientos del PSVA. b) La generación de la clave de firma de la Unidad de Sello de Tiempo deberá ser realizada en un módulo criptográfico que: • Cumpla con los requerimientos FIPS 140-2 nivel 3 o superior o • Cumpla los requerimientos identificados en el CEN Workshop Agreement 14167-2 (CWA 14167-2) o c) El algoritmo de generación, la longitud de la clave firma y el algoritmo de firma usado para firmar los sellos de tiempo deberán ser	Ejemplos de evidencias que deben ser requeridas: • Acta y procedimiento de generación u otro documento donde se especifican las condiciones técnicas y procedimientos vinculados a la generación de la clave TSU, así como la identificación del personal de confianza encargado y su nombramiento • Documento donde se identifican los módulos criptográficos empleados y la evidencia de las certificaciones de seguridad correspondientes • Documentación o evidencia donde se especifiquen el algoritmo de generación de las claves de la TSU, el tamaño de la clave y los algoritmos de firma, los cuales deben ser reconocidos por la IOFE • Documento donde se especifiquen los roles de confianza participantes, las responsabilidades y su debida asignación • Inspección visual del ambiente físico seguro donde se genera la clave de la TSU

		reconocidos por la IOFE. La lista de estándares criptográficos recomendados se lista en el estándar ETSI TS 102 176 -1, a excepción de los algoritmos de generación de claves RSA 1024 y los HASH MD5 y SHA-1.	
17	Protección de la clave privada de la TSU	La TSA debe asegurar que la clave privada de firma permanece confidencial y que se mantiene su integridad a) La clave de firma de la Unidad de Sello de Tiempo deberá ser protegida en un módulo criptográfico que: • Cumpla con los requerimientos FIPS 140-2 nivel 3 o superior o • Cumpla los requerimientos identificados en el CEN Workshop Agreement 14167-2 (CWA 14167-2) b) Si se realiza un respaldo de la clave de firma de la Unidad de Sello de tiempo, esta deberá ser copiada, almacenada y recuperada sólo por	Ejemplos de evidencias que deben ser requeridas: • Acta y procedimiento de protección para el almacenamiento de las copias de respaldo fuera del módulo criptográfico • Inspección visual del módulo criptográfico que está interconectado en el sistema de producción de los sellos de tiempo.

		personal que ocupa roles de confianza, usando al menos el control de acceso de dos personas. El personal autorizado para realizar estas funciones debe estar limitado para realizar esta tarea conforme a los procedimientos del PSVA. c) Cualquier copia de la TSU deberá ser protegida por la clave secreta del módulo criptográfico antes de ser almacenada fuera del dispositivo	
18	Distribución de la clave pública TSU	La clave pública de firma de la TSU debe ser disponible para los terceros que confían en un certificado de clave pública. El certificado puede ser emitido por la misma entidad que opera la TSA o por otra EC reconocida por la IOFE. El certificado de la Unidad de sello de tiempo debe ser emitido por una EC bajo una política que provea un nivel de seguridad equivalente o superior a la Política de Sellado de Tiempo. Este certificado deberá ser reconocido por la IOFE	Ejemplos de evidencias: • Procedimiento de distribución de la clave pública de la TSU • Certificado digital que contiene la clave pública de la TSU • Certificación que ampara la seguridad del certificado digital

19	Re-emisión de la clave del TSU	El tiempo de vigencia del certificado de la TSU no debe ser mayor que el periodo de vigencia de los algoritmos y tamaños de claves, conforme al reconocimiento de la IOFE.	Ejemplos de evidencias: • Documentación donde se especifiquen las características técnicas referidas a la re-emisión de la clave de la TSU
20	Término del ciclo de vida de la clave privada del TSU	La TSA debe asegurar que las claves privadas de firma de la TSU no son usadas luego de expirado su ciclo de vida: a) Se deben establecer procedimientos técnicos u operacionales para asegurar que son generadas y utilizadas nuevas claves b) La clave privada de firma, o cualquier parte de la clave debe ser destruida de tal modo que no pueda ser recuperada c) El sistema de generación de sellos de tiempos debe rechazar cualquier intento de emitir sellos de tiempo si la clave privada de firma ha expirado o se encuentra revocada.	Ejemplos de evidencias: • Procedimiento de gestión de la clave de la TSU luego de su expiración o revocación: • Emisión de una nueva clave • Destrucción de la clave expirada o revocada, incluyendo cualquier copia • Impedimento de emisión de sello de tiempo

2.3. Ciclo de vida del módulo criptográfico usado para firma sellos de tiempo

Ciclo de vida del módulo criptográfico			
Explicación preliminar: El PSVA debe proteger el módulo criptográfico donde se almacena su clave privada, a fin de evitar su compromiso.			
No	Requerimiento		Detalle
21	Gestión del ciclo de vida del módulo criptográfico usado para firmar los sellos de tiempo	a) El hardware del módulo criptográfico no debe ser manipulado durante su transporte b) El hardware del módulo criptográfico no debe ser manipulado durante su almacenamiento c) La instalación, activación y duplicación de la clave de firma de la TSU en el hardware del módulo criptográfico deberá ser realizado solo por personal que ocupa roles de confianza, usando al menos un control de acceso de dos personas en un ambiente físico seguro. d) El hardware de firma de sellos de tiempo funciona correctamente	Ejemplos de evidencias • Procedimiento de gestión del módulo criptográfico Pruebas de aseguramiento de correcto funcionamiento del equipo Registros de borrado de claves privadas de la TSU antes de que el equipo sea desechado

		e) Las claves de firma de la TSU que son almacenadas en un módulo criptográfico son borradas antes de que el dispositivo sea retirado	

2.4. Sello de Tiempo

Sello de tiempo			
Explicación preliminar: El sello de tiempo debe contener ciertos datos que permitirán su verificación y vinculación con la TSA.			
No	Requerimiento		Detalle
22	Sellado de Tiempo	El sello de tiempo: • Debe incluir un identificador de la política de sellado de tiempo • Debe tener un único identificador • El valor de tiempo debe ser trazable a al menos una fuente de tiempo confiable reconocida por el Bureau International des Poids et Mesures (BIPM) • El tiempo definido debe ser sincronizado con la fuente de tiempo confiable dentro de la exactitud definida en la Política de Sellado de tiempo, así como dentro	

		de la exactitud definida en el mismo sello de tiempo • Si el tiempo provisto se encuentra fuera de la exactitud definida el sello de tiempo no debe ser emitido • Debe incluir un resumen de los datos firmados (por ejemplo, hash) • El sello de tiempo debe ser firmado por una clave generada para este propósito • Debe incluir, si fuera aplicable: o un identificador para el país en el cual la TSA es establecida o Debe incluir un identificador para la TSA o Debe incluir un identificador para la TSU que emite los sellos de tiempo	

2.5. Sincronización del reloj con el UTC

Sincronización del reloj			
Explicación preliminar: El PSVA debe mantener la sincronización del reloj de la TSU con la UTC.			
No	Requerimiento		Detalle
23	Sincronización con la UTC	• La calibración de los relojes de la TSU debe ser mantenida de modo que no supere la exactitud declarada • Los relojes deben ser protegidos contra amenazas como cambios no autorizados que afecten la calibración • La TSA deberá asegurar que si el tiempo indicado en el sello de tiempo excede la sincronización con la UTC, esto será detectado. Los terceros de confianza deben ser notificados. • La TSA deberá asegurar que la sincronización del reloj es mantenida cuando un salto de segundo es definido por la autoridad respectiva. El cambio debe tener en cuenta que el salto de segundo debe ocurrir durante el último minuto del último día de su planificación. Un registro de este cambio debe ser mantenido.	Ejemplos de evidencias: • Verificación del sello de tiempo • Verificación de la fuente de tiempo confiable • Documentos de calibración del reloj o documentación del servidor de tiempo • Procedimientos de contingencia • Procedimiento de gestión del reloj de la TSU: • Mantener el reloj dentro de la precisión declarada • Protección del reloj contra amenazas luego de la calibración • Aseguramiento de la sincronización del reloj ante un cambio en el tiempo notificado por una autoridad competente

2.6. Gestión de la seguridad

Gestión de la seguridad			
Explicación preliminar: El PSVA debe implementar los controles necesarios para asegurar la información en sus operaciones			
No	Requerimiento		Detalle
24	Organización de la seguridad de la información	Debe existir un responsable de organizar y dirigir la seguridad de la información	
25	Política de seguridad de la información	Se debe implementar y establecer una Política de seguridad cuyo alcance cubra todas las operaciones críticas del SVA El PSVA deberá asegurar la publicación de esta política y comunicación a todos los empleados que participan de las operaciones del SVA.	
26	Gestión de riesgos	Los riesgos de seguridad deben ser evaluados periódicamente y los controles a ser implementados deben ser conformes a las amenazas y riesgos detectados.	
27	Documentación	Los procedimientos operativos y de seguridad deben ser documentados.	

28	Seguridad en el trato con terceros	• La seguridad debe ser mantenida cuando las funciones son tercerizadas a otra organización o entidad. El PSVA es responsable de los servicios que brinda, incluyendo los que son realizados por terceros proveedores • Las responsabilidades de terceros deben ser definidas y deben hacerse arreglos para asegurar que los terceros cumplen todos los controles requeridos • El PSVA deberá mantener la responsabilidad de declarar las prácticas relevantes de tercerización a todas las partes interesadas	
29	Clasificación y gestión de activos	El PSVA deberá mantener un inventario de todos los activos críticos, asignando una clasificación de sus requerimientos de protección, de manera consistente con el análisis de riesgos	Ejemplo de evidencia: Documento donde se establece la clasificación y gestión de activos
30	Seguridad del personal	a) El PSVA deberá emplear personal que posea conocimiento especializado, experiencia y calificaciones necesarias para ofrecer los servicios, de acuerdo a las	

		funciones que debe cumplir cada rol b) Los roles y responsabilidades referidas al cumplimiento de la Política de Seguridad, deben ser documentados en las descripciones de las funciones de cada rol. Los roles de confianza, de los cuales dependen las operaciones del SVA deberán ser identificados. c) Las funciones del personal del SVA (temporal y permanente) deberán definidas considerando los criterios de separación de derechos y mínimo privilegio d) El personal deberá ejecutar sus funciones y procedimientos en función de los procedimientos y la Política de Seguridad. e) El personal gerencial debe tener conocimiento de las tecnologías relacionadas a los servicios del SVA, como firma digital, gestión de certificados digitales, sello de tiempo, mecanismos de sincronización de relojes con la UTC,	

		conocimientos de los procedimientos y responsabilidades de seguridad para la gestión de personal, experiencia en seguridad de la información y evaluación de riesgos. f) Todo el personal en roles de confianza debe ser libre de conflicto de interés que pueda perjudicar la imparcialidad de las operaciones del SVA g) Los roles de confianza deben incluir las siguientes responsabilidades: • Oficiales de seguridad: Responsables de administrar la implementación de las prácticas de seguridad • Administradores de sistemas: Autorizados a instalar, configurar y mantener la integridad de los sistemas del SVA • Operadores de sistemas: Responsable de operar la integridad de los sistemas en el día a día. Autorizados para ejecutar sistemas de respaldo y recuperación.	

		• Auditores de sistemas: Autorizados a ver archivos y logs de los sistemas del SVA h) El personal debe ser formalmente asignado a cumplir los roles de confianza, por parte del responsable gerencial de la seguridad i) El PSVA no deberá asignar en roles de confianza o administración a cualquier persona que es conocida por tener una participación en un crimen serio u otra ofensa la cual afecta su idoneidad para su puesto. El personal no deberá tener acceso a funciones de confianza hasta completar todas las verificaciones necesarias.	
31	Seguridad física y del entorno	a) Los medios de administración de los sistemas del SVA deberán ser operados en un ambiente protegido con controles físicos de acceso para proteger de acceso no autorizado a los sistemas y datos b) Se deben definir perímetros de seguridad que protejan las operaciones y sistemas críticos del SVA. Las partes compartidas con otras organizaciones deberán ser afuera de este perímetro.	Ejemplos de evidencias: Inspección visual de la implementación de: • Acceso físico limitado apropiadamente a individuos autorizados • Operación de medios de procesamiento desde ambiente con protección física • Controles contra pérdida, daños o compromiso de los activos de información, así como interrupción de las actividades del negocio • Controles contra compromiso o robo de información y sus medios de procesamiento

		c) Controles de seguridad física y ambiental deben ser implementados para proteger los medios que alojan los recursos informáticos, los recursos informáticos, y los medios usados para soportar su operación. Estos deben incluir: protección de acceso físico, protección contra desastres naturales, detección y protección contra incendios, contingencia en cortes de energías y comunicaciones, colapso de la estructura, aniego, protección contra robo, ruptura, recuperación en caso de desastres, conforme a los resultados del análisis de riesgos. d) Se deben implementar controles que impidan el retiro no autorizado de equipos, información, medios de almacenamiento, software relativo a los servicios críticos del SVA.	• Controles de seguridad ambientales (controles contra incendio, regulación de humedad, temperatura)
32	Gestión de operaciones	a) La integridad de los componentes informáticos y la información deben ser protegidos contra virus, software malicioso o no autorizado. b) Se deben implementar y ejecutar procedimientos de reporte y respuestas a incidentes de seguridad y mal funcionamiento de las operaciones del SVA	

		c) Los medios de almacenamiento usados en los sistemas críticos del SVA deben ser protegidos contra modificación o acceso no autorizados d) Se deben establecer procedimientos para todos los roles de confianza y administrativos que impactan en la provisión de servicios del SVA. e) Se deben implementar procedimientos para asegurar la adecuada planificación de activos y nuevos sistemas a fin de evitar incompatibilidades con otros sistemas y vulnerabilidades de seguridad f) La limpieza de los ambientes debe ser adecuada para no dañar los equipos, y el personal debe ser supervisado para evitar robos de medios de almacenamiento e información	
33	Manejo de medios y seguridad	Todos los medios deben ser manejados de manera segura conforme a la clasificación de activos. Los medios de almacenamiento que contienen datos sensibles deben ser eliminados de manera segura cuando ya no sean requeridos.	

34	Planificación del sistema	Las demandas de capacidad de los sistemas deben ser monitoreadas y deben realizarse proyecciones de la demanda futura a fin de asegurar la disponibilidad de los sistemas de procesamiento y almacenamiento.	
35	Reporte y respuesta a incidentes	El PSVA debe actuar de manera oportuna y coordinada para responder de manera rápida a los incidentes y limitar el impacto de los vacíos de seguridad. Todos los incidentes deben ser reportados tan pronto como sea posible.	Ejemplos de evidencias: Reportes de incidentes, informes de seguimiento y solución Estadísticas de incidentes reportados y atendidos
36	Seguridad en redes	• Debe definirse una política de acceso en redes • Las redes deben ser protegidas de acceso no autorizado, • Se debe separar la zona de constante acceso con la red interna de procesamiento y almacenamiento de información crítica. De acuerdo a los diferentes niveles de seguridad, deben separarse las redes de datos de los sistemas de procesamiento central del SVA • El acceso a dominios de redes internas del SVA deben ser protegidos de acceso o autorizado incluyendo a suscriptores y terceros que confían. Los firewalls deben ser	

		configurados para prevenir todos los protocolos y accesos no requeridos para la operación del SVA • Deben implementarse sistemas de detección de intrusos para prevenir accesos de código malicioso o no autorizado	
37	Monitoreo	• La continuidad y seguridad de las operaciones debe ser monitoreada. • Los registros de auditoría y los reportes de eventos sobre errores y advertencias en el funcionamiento de los sistemas del SVA deben ser monitoreados • Medios de monitoreo y alarmas deben ser implementados para detectar, registrar y actuar oportunamente sobre accesos no autorizados o intentos irregulares de acceso a recursos.	
38	Intercambio de datos y software	Se debe evaluar las vulnerabilidades y riesgos de seguridad relacionados al intercambio de datos y software, y estos deben ser manejados de manera apropiada de acuerdo a su impacto sobre las operaciones del SVA	

39	Gestión de accesos a los sistemas	El SVA debe asegurar que el acceso a los sistemas es limitado a individuos autorizados apropiadamente: • Se debe realizar una efectiva administración de accesos de usuarios (operadores, administradores y auditores), a sistemas que mantienen la seguridad del SVA. Esta gestión debe incluir una asignación de cuentas de usuario, auditoria, modificación o remoción oportuna de acceso. • El personal debe ser apropiadamente identificado y autenticado antes de tener acceso a aplicaciones críticas del SVA • El personal debe ser controlado respecto de las acciones que realiza en los sistemas del SVA, mediante registros de auditoria.	
40	Archivo	La información crítica y sensible, que es archivada debe ser protegida contra daño ambiental o intencional, así como acceso de lectura y modificación no autorizadas.	Ejemplo de evidencia: Procedimiento de gestión del archivo.
41	Desarrollo y mantenimiento	Se debe realizar un análisis de los requerimientos de seguridad que deben ser	Ejemplos de evidencias:

	de sistemas confiables	cubiertos en las etapas de diseño y especificación de los proyectos de desarrollo de sistemas del SVA, para asegurar que dichos requerimientos son considerados en los sistemas críticos	Documento donde se establece el análisis de requerimientos de seguridad en la etapa de diseño y especificación de requerimientos de todo proyecto de desarrollo realizado por o en nombre de la TSA
42	Control de cambios	Se debe implementar procedimientos de control de cambios para poner en producción modificaciones o parches de emergencia de aplicaciones críticas de software del SVA, a fin de evitar posteriores fallas o incompatibilidad con otros sistemas.	Ejemplo de evidencias: Procedimientos de control de cambios

2.7. Compromiso de los servicios de la TSA o TSU

Compromiso de la TSA			
Explicación preliminar: El PSVA debe adoptar los procedimientos de contingencia necesarios en caso de compromiso de sus servicios.			
No	Requerimiento		Detalle
43	Recuperación de desastres	La TSA debe implementar un plan de recuperación de desastres que considere los casos: • Sospecha de compromiso de la clave privada de firma del TSU o • La pérdida de calibración del reloj, los cuales pueden	

		afectar los sellos de tiempo que ha sido emitidos.	
44	Notificación	En el caso de compromiso de las operaciones de la TSA, por sospecha de compromiso de la clave privada de firma o pérdida de la calibración de los sellos de tiempo, la TSA debe hacer disponible a todos los suscriptores y terceros que confían una descripción del compromiso ocurrido	
45	Interrupción de operaciones	En el caso de compromiso de las operaciones de la TSA, por sospecha de compromiso de la clave privada de firma o pérdida de la calibración de los sellos de tiempo, no deberán ser emitidos sellos de tiempo hasta que se logre recuperar las operaciones del compromiso	En caso de compromiso de la clave privada de firma, no se podrán emitir sellos de tiempo hasta que sea emitida una nueva clave y se garantice su seguridad. En caso de pérdida de la calibración del reloj, no se podrán emitir sellos de tiempo hasta que se haya recuperado la calibración.
46	Mecanismos de verificación para terceros que confían	En el caso de compromiso de las operaciones de la TSA, por sospecha de compromiso de la clave privada de firma o pérdida de la calibración de los sellos de tiempo, la TSA deberá poner a disponibilidad de todos los suscriptores y terceros que confían información sobre el mecanismo que puede ser usado para identificar los	Ejemplos de evidencias: • Procedimiento de gestión del término de los servicios de la TSA: • Comunicación a suscriptores y terceros que confían • Terminar las autorizaciones de los subcontratados

		sellos de tiempo que han sido comprometidos, a menos que afecte una brecha de privacidad de los usuarios de los sellos de tiempo o genere una brecha en la seguridad de los servicios de la TSA.	• Transferencia de obligaciones a un tercero confiable • Destrucción de las claves privadas de las TSU • Revocación de los certificados digitales de las TSU

2.8. Término de la organización que administra la TSA

Término de la TSA		
Explicación preliminar: El SVA debe adoptar las medidas necesarias para que su finalización no afecte de manera significativa a los suscriptores y terceros que confían.		
No	Requerimiento	Detalle
47	Preparación antes del término	a) La TSA debe poner a disponibilidad de los suscriptores y terceros que confían la información concerniente a su terminación b) La TSA deberá terminar con las autorizaciones de todos los subcontratistas que actúan en nombre de la TSA, en el proceso de emisión de los sellos de tiempo c) La TSA deberá transferir sus obligaciones a una parte confiable para mantener los archivos de los log de eventos y	Acuerdos para cubrir los costos mínimos, en caso se declare la quiebra u otras razones que le impidan cubrir los costos

		registros de auditorías necesarios para demostrar la correcta operación de la TSA por un periodo razonable d) La TSA deberá transferir sus obligaciones a una parte confiable para mantener disponible su clave pública o sus certificados a los terceros que confían por un periodo razonable de tiempo e) Las claves privadas de TSU incluyendo las copias de respaldo deberán ser destruidos de tal manera que la clave privada no pueda ser recuperada	
48	Capacidad financiera	La TSA deberá tener un arreglo para cubrir los costos que implica implementar estos requerimientos mínimos en caso que la TSA quiebre financieramente o por otras razones que inhabiliten su capacidad de cubrir los costos por sí misma.	
49	Revocación del certificado de la TSA	La TSA deberá adoptar los pasos necesarios para revocar los certificados de la TSU	

2.9. Registros de información concerniente a la operación de los servicios de sellado de tiempo

Registros de auditoría			
Explicación preliminar: El PSVA debe registrar los eventos que sean necesarios como evidencia legal de la confiabilidad de los servicios brindados.			
No	Requerimiento		Detalle
50	Eventos registrados	La TSA debe declarar los tipos de eventos y datos que serán registrados	
51	Protección de los registros	La confidencialidad e integridad los registros vigentes y los archivados concernientes a la operación de los servicios de sellos de tiempo debe ser mantenida. Los eventos deben ser registrados en un modo que ellos no puedan ser borrados o destruidos dentro del periodo de tiempo que son requeridos como evidencia (excepto si son transferidos a medios de almacenamiento de largo plazo).	
52	Archivo de registros	Los registros concernientes a la operación de los servicios de sello de tiempo deberán ser archivados de manera completa y confidencial en concordancia con la DPSVA	

53	Eventos significativos	Debe ser registrado el tiempo preciso en el que ocurren eventos significativos en los ambientes, gestión de claves o sincronización del reloj.	
54	Evidencias legales	Registros concernientes a la operación de sellos de tiempo deberán ser disponibles si es requerido para propósitos de proveer evidencia de la correcta operación de los servicios de sello de tiempo para propósitos legales	
55	Archivo luego de expiración de la TSA	Los registros concernientes a los sellos de tiempo deberán ser mantenidos por un periodo de tiempo después de la expiración de la vigencia de las claves de firma de la TSU	
56	Privacidad	Cualquier información que es registrada acerca de los suscriptores deberá ser guardada de manera confidencial excepto si se obtiene el consentimiento del suscriptor para su publicación	
57	Gestión de la clave de la TSU	Se deben registrar eventos relacionados al ciclo de vida de la clave privada de la TSU	
58	Registros de Sincronización del reloj	Se deben registrar todos los eventos relacionados a la sincronización de los relojes del TSU a la UTC. Esto deberá incluir información concerniente a la re-calibración normal o	

		sincronización de los relojes usados en el sello de tiempo Se deben registrar todos los eventos relacionados con la pérdida de sincronización de los relojes con la UTC	

2.10. Auditoria

Auditoría			
Explicación preliminar: El PSVA debe ser auditada anualmente por la AAC, respecto de la correcta operación de los servicios de registro.			
No	Requerimiento		Detalle
59	Auditoría de registros	Los registros deben ser revisados como parte de la auditoría de la AAC, de manera anual.	
60	Auditoría del archivo	El archivo debe ser revisados como parte de la auditoría de la AAC, de manera anual.	
61	Auditoría de los procedimientos y controles	Los procedimientos y controles implementados deben ser auditados por la AAC de manera anual.	

62	Auditor	El auditor debe: • Ser autorizado por la AAC. • Ser independiente del PSVA, y no haber realizado trabajos para ella dentro de los 2 años anteriores a la ejecución de la auditoría.	

2.11. Otros aspectos legales de la operación de la TSA

Aspectos legales de la operación del TSA			
Explicación preliminar:			
No	Requerimiento		Detalle
63	Políticas de reembolso	El PSVA debe declarar, si fuera aplicable, políticas de reembolso, incluyendo los siguientes casos, indicar donde el cliente puede ser informado respecto, de las políticas de reembolso del servicio.	
64	Cobertura de seguro de responsabilidad civil	El monto mínimo de la póliza es de $ 35 000. 00 dólares americanos. El PSVA debe publicar las garantías financieras que ofrece a los terceros que confían en caso de ocurrir suplantación de	

		identidad por fallos en la operación del SVA.	
65	Información confidencial y/o privada	El PSVA debe mantener de manera confidencial la siguiente información: • Material comercialmente reservado de los PSCs, de los suscriptores de la empresa y de los 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.	
66	Información no privada	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.	
67	Derechos de Propiedad intelectual	De ser aplicable, el SVA debe declarar cláusulas contractuales de respecto de obligaciones y derechos relacionados a la propiedad intelectual.	
68	Notificaciones y comunicaciones entre participantes	El PSVA debe declarar los mecanismos de comunicación con sus clientes, en orden de realizar comunicaciones con valor legal.	
69	Conformidad con la Ley aplicable	El PSVA debe declarar la ley aplicable que debe ser cumplida por los participantes.	

70	Exención de garantías	En caso de existir, el PSVA debe declarar los casos de exención de garantías aplicables	
71	Indemnizaciones	En caso de existir, el PSVA debe declarar las indemnizaciones aplicables	
72	Fuerza mayor	En caso de existir, el PSVA debe declarar en algún documento normativo, las cláusulas de fuerza mayor que sean aplicables.	

3. SISTEMAS DE INTEMEDIACIÓN DIGITAL

3.1. SISTEMAS DE INTERMEDIACIÓN DIGITAL COMO PRODUCTO

Una característica importante de este SVA, es que se trata de productos de software y/o hardware y no servicios, por lo que se asume que no se realiza un almacenamiento de datos, ni se almacena o protege una clave privada.

Los SVA tipo Sistemas de Intermediación Digital como Producto deben ser evaluados respecto del cumplimiento de los requerimientos descritos en la sección 8 y anexo I del presente documento.

3.1.1. Definición de Responsabilidades

Responsabilidades		
Explicación preliminar: Se deben definir las responsabilidades de las partes.		
No	Requerimiento	Detalle

1	Responsabilidades y obligaciones del PSVA	El PSVA deberá definir sus responsabilidades en relación con los usuarios de los sistemas del SVA	
2	Responsabilidades y obligaciones del suscriptor	El PSVA deberá definir las responsabilidades de los suscriptores, usuarios de los sistemas de intermediación digital como Producto	
3	Responsabilidades de los Terceros que confían	El PSVA deberá definir las responsabilidades de los terceros que confían, incluyendo: • Verificar la validez de los certificados digitales de los documentos o información procesada por los sistemas de intermediación digital como Producto • Tomar en cuenta cualquier limitación en el uso de los sistemas considerados en la DPSVA • Tomar en cuenta cualquier otra precaución prescrita en los acuerdos u otra parte.	
4	Responsabilidades	La TSA puede declarar o limitar cualquier responsabilidad excepto aquellas que sean estipuladas en la regulación vigente.	

5	Resolución de disputas	El PSVA debe establecer procedimientos para la resolución de disputas con sus clientes, indicando los datos de contacto o dirección a donde pueden dirigirse los reclamos.	

3.1.2. Módulo criptográfico

Módulo criptográfico			
Explicación preliminar: En caso que los sistemas se integren a un módulo criptográfico, éste deberá cumplir con requerimientos que garanticen la seguridad de la clave privada que los suscriptores utilizarán.			
No	Requerimiento		Detalle
6	Certificaciones de Seguridad	El modulo criptográfico debe cumplir con la certificación • FIPS 140-2 o • Cumplan los requerimientos identificados en el CEN Workshop Agreement 1167-2 (CWA 14167-2)	

3.1.3. Autenticación

Autenticación			
Explicación preliminar: En caso que los sistemas contemplen funciones de validación de identidad de sus usuarios mediante un certificado digital, deberán verificar la validez del mismo antes de autorizar su acceso.			
No	Requerimiento		Detalle
7	Validación de la confiabilidad de la raíz	El sistema deberá verificar que el certificado corresponde a una Entidad de Certificación reconocida por la IOFE, de no ser exitosa la verificación, el sistema no debe permitir el acceso.	
8	Validación del estado de revocación	El sistema deberá verificar que tanto el certificado del usuario final, así como los certificados que componen la cadena de certificación no se encuentran revocados. Esta verificación puede ser mediante los mecanismos CRL u OCSP. En caso de ser CRL, se deberá verificar la vigencia y autenticidad de la CRL.	La autenticidad de la CRL se verifica mediante la verificación de la firma, buscando que haya sido realizada por la EC que emitió la CRL.

9	Validación del estado de vigencia	El sistema deberá verificar que tanto el certificado del usuario final así como los certificados que componen la cadena de certificación se encuentran vigentes, es decir, que su periodo de vida no ha expirado.	
10	Validación del propósito	El sistema deberá verificar que el certificado del usuario final tiene como propósito autenticación, conforme a la RFC 5280.	

3.1.4. Cifrado

Cifrado		
Explicación preliminar: En caso que los sistemas realicen funciones de cifrado con certificados digitales, se deberá proteger la clave privada empleada en los procesos de cifrado		
No	Requerimiento	Detalle
11	Protección de la clave privada	Al momento de descifrar la información, el sistema no deberá copiar la clave privada sin cifrar fuera del módulo criptográfico. La clave privada siempre debe mantenerse dentro del módulo criptográfico.

12	Validación de la confiabilidad de la raíz	El sistema deberá verificar que el certificado corresponde a una Entidad de Certificación reconocida por la IOFE, de no ser exitosa la verificación, el sistema no debe permitir el acceso.	
13	Validación del estado de revocación	El sistema deberá verificar que tanto el certificado del usuario final, así como los certificados que componen la cadena de certificación no se encuentran revocados. Esta verificación puede ser mediante los mecanismos CRL u OCSP. En caso de ser CRL, se deberá verificar la vigencia y autenticidad de la CRL.	La autenticidad de la CRL se verifica mediante la verificación de la firma, buscando que haya sido realizada por la EC que emitió la CRL.
14	Validación del estado de vigencia	El sistema deberá verificar que tanto el certificado del usuario final, así como los certificados que componen la cadena de certificación se encuentran vigentes, es decir, que su periodo de vida no ha expirado.	
15	Validación del propósito	El sistema deberá verificar que el certificado del usuario final tiene como propósito de cifrado o cifrado de clave, conforme a la RFC 5280.	

3.1.5. Canales SSL

Canales SSL			
Explicación preliminar: En caso que los sistemas implementen canales seguros SSL			
No	Requerimiento		Detalle
16	Protección de la clave privada	Al momento de descifrar la información, el sistema no deberá copiar la clave privada sin cifrar fuera del módulo criptográfico. La clave privada siempre debe mantenerse dentro del módulo criptográfico.	
17	Validación de la confiabilidad de la raíz	El sistema deberá verificar que el certificado corresponde a una Entidad de Certificación reconocida por la IOFE, de no ser exitosa la verificación, el sistema no debe permitir el acceso.	
18	Validación del estado de revocación	El sistema deberá verificar que tanto el certificado del usuario final, así como los certificados que componen la cadena de certificación no se encuentran revocados. Esta verificación puede ser mediante los mecanismos CRL u OCSP. En caso de ser CRL, se deberá verificar la vigencia y autenticidad de la CRL.	La autenticidad de la CRL se verifica mediante la verificación de la firma, buscando que haya sido realizada por la EC que emitió la CRL.

19	Validación del estado de vigencia	El sistema deberá verificar que tanto el certificado del usuario final, así como los certificados que componen la cadena de certificación se encuentran vigentes, es decir, que su periodo de vida no ha expirado.	
20	Validación del propósito	El sistema deberá verificar que el certificado del usuario final tiene como propósito de cifrado de clave, conforme a la RFC 5280.	

3.1.6. Consulta de sellos de tiempo

Consulta de sellos de tiempo			
Explicación preliminar: En caso que los sistemas realicen peticiones de sellos de tiempo, deben cumplir requisitos que garanticen su confiabilidad			
No	Requerimiento		Detalle
21	Formato de petición	El formato de petición debe ser conforme a la RFC 3161.	
22	Validación de la confiabilidad de la raíz	El sistema deberá verificar que el certificado con el que se firma el sello de tiempo corresponde a una Entidad de Certificación reconocida por la IOFE.	

23	Validación del estado de revocación	El sistema deberá verificar que el certificado con el que se firman los sellos de tiempo no se encuentra revocado.	
24	Validación del estado de vigencia	El sistema deberá verificar que el certificado con el que se firman los sellos de tiempo no se encuentra expirado.	
25	Validación de la firma	El sistema deberá verificar la firma del sello de tiempo para corroborar que los datos son íntegros	

3.1.7. Gestión de la seguridad

Gestión de la seguridad			
Explicación preliminar: El PSVA debe implementar los controles necesarios para asegurar la información en sus operaciones			
No	Requerimiento		Detalle
26	Organización de la seguridad de la información	Debe existir un responsable de organizar y dirigir la seguridad de la información	
27	Política de seguridad de la información	Se debe implementar y establecer una Política de seguridad cuyo alcance cubra	

		todas las operaciones críticas del SVA El PSVA deberá asegurar la publicación de esta Política y comunicación a todos los empleados que participan de las operaciones del SVA.	
28	Seguridad en el trato con terceros	• La seguridad debe ser mantenida cuando las funciones son tercerizadas a otra organización o entidad. El PSVA es responsable de los servicios que brinda, incluyendo los que son realizados por terceros proveedores • Las responsabilidades de terceros deben ser definidas y deben hacerse arreglos para asegurar que los terceros cumplen todos los controles requeridos • El PSVA deberá mantener la responsabilidad de declarar las prácticas relevantes de tercerización a todas las partes interesadas	
29	Seguridad del personal	a) El PSVA deberá emplear personal que posea conocimiento especializado, experiencia y calificaciones	

		necesarias para ofrecer los servicios, de acuerdo a las funciones que debe cumplir cada rol b) Los roles y responsabilidades referidas al cumplimiento de la Política de Seguridad, deben ser documentados en las descripciones de las funciones de cada rol. Los roles de confianza, de los cuales dependen las operaciones del SVA deberán ser identificados. c) Las funciones del personal del SVA (temporal y permanente) deberán definidas considerando los criterios de separación de derechos y mínimo privilegio d) El personal deberá ejecutar sus funciones y procedimientos en función de los procedimientos y la Política de Seguridad. e) El personal gerencial debe tener conocimiento de las tecnologías relacionadas a los servicios del SVA, como firma digital, gestión de certificados digitales, sello de tiempo,	

		mecanismos de sincronización de relojes con la UTC, conocimientos de los procedimientos y responsabilidades de seguridad para la gestión de personal, experiencia en seguridad de la información y evaluación de riesgos. f) Todo el personal en roles de confianza debe ser libre de conflicto de interés que pueda perjudicar la imparcialidad de las operaciones del SVA g) Los roles de confianza deben incluir las siguientes responsabilidades: • Oficiales de seguridad: Responsables de administrar la implementación de las prácticas de seguridad • Administradores de sistemas: Autorizados a instalar, configurar y mantener la integridad de los sistemas del SVA • Operadores de sistemas: Responsable de operar la integridad de los sistemas en el día a día. Autorizados para	

		ejecutar sistemas de respaldo y recuperación. • Auditores de sistemas: Autorizados a ver archivos y logs de los sistemas del SVA h) El personal debe ser formalmente asignado a cumplir los roles de confianza, por parte del responsable gerencial de la seguridad i) El PSVA no deberá asignar en roles de confianza o administración a cualquier persona que es conocida por tener una participación en un crimen serio u otra ofensa la cual afecta su idoneidad para su puesto. El personal no deberá tener acceso a funciones de confianza hasta completar todas las verificaciones necesarias.	
30	Gestión de accesos a los sistemas	En caso que el sistema se encuentre integrado a un sistema de gestión de usuarios, este deberá cumplir lo siguiente: • Permitir la asignación de cuentas de usuario para controlar los accesos a los sistemas, permitir la modificación o remoción oportuna de accesos. • Diferenciar las cuentas de administración de las cuentas de usuario.	

		• El sistema debe permitir controlar al personal respecto de las acciones críticas que realiza en los sistemas del SVA, generando registros de auditoria.	
31	Desarrollo y mantenimiento de sistemas confiables	Se debe realizar un análisis de los requerimientos de seguridad que deben ser cubiertos en las etapas de diseño y especificación de los proyectos de desarrollo de sistemas del SVA, para asegurar que dichos requerimientos son considerados en los sistemas críticos	Ejemplos de evidencias: Documento donde se establece el análisis de requerimientos de seguridad en la etapa de diseño y especificación de requerimientos de todo proyecto de desarrollo realizado por o en nombre del PSVA

3.1.8. Término de la organización que administra el SVA

Término del SVA		
Explicación preliminar: El SVA debe adoptar las medidas necesarias para que su finalización no afecte de manera significativa a los suscriptores y terceros que confían.		
No	Requerimiento	Detalle
32	Preparación antes del término	a) El PSVA debe poner a disponibilidad de los suscriptores y terceros que confían la información concerniente a su terminación b) El PSVA deberá terminar con las autorizaciones de todos los subcontratistas	Acuerdos para cubrir los costos mínimos, en caso se declare la quiebra u otras razones que le impidan cubrir los costos

		que actúan en nombre del PSVA c) Asegurar el cumplimiento o compensación por los servicios comprometidos de soporte o garantía	

3.1.9. Registros de auditoría

Registros de auditoría			
Explicación preliminar: El sistema debe permitir registrar los eventos críticos			
No	Requerimiento		Detalle
33	Eventos registrados	El PSVA debe declarar los tipos de eventos y datos que serán registrados. Los eventos que deben ser registrados deben ser relacionados a las transacciones de autenticación y generación de firma digital.	
34	Protección de los registros	Los eventos deben ser registrados en un modo que ellos no puedan ser borrados o destruidos dentro del periodo de tiempo que son requeridos como evidencia (excepto si son transferidos a medios de almacenamiento de largo plazo).	
35	Eventos significativos	Deben ser registradas las solicitudes o transacciones de firma digital, autenticación o cifrado	

3.1.10. Auditoría

Auditoría			
Explicación preliminar: El PSVA debe ser auditada anualmente por la AAC, respecto de la correcta operación de los servicios de registro.			
No	Requerimiento		Detalle
36	Auditoría de registros	Los registros deben ser revisados como parte de la auditoría de la AAC, de manera anual.	
37	Auditoría del archivo	El archivo debe ser revisado como parte de la auditoría de la AAC, de manera anual.	
38	Auditoría de los procedimientos y controles	Los procedimientos y controles implementados deben ser auditados por la AAC de manera anual.	
39	Auditor	El auditor debe: • Ser autorizado por la AAC. • Ser independiente del PSVA, y no haber realizado trabajos para ella dentro de los 2 años anteriores a la ejecución de la auditoría.	

3.1.11. Aspectos Legales de la operación del PSC

Aspectos legales de la operación del PSC			
Explicación preliminar:			
No	Requerimiento		Detalle
40	Políticas de reembolso	El PSVA debe declarar, si fuera aplicable, políticas de reembolso, incluyendo los siguientes casos, indicar donde el cliente puede ser informado respecto, de las políticas de reembolso del servicio.	
41	Cobertura de seguro de responsabilidad civil	El monto mínimo de la póliza es de $ 35 000. 00 dólares americanos. El PSVA debe publicar las garantías financieras que ofrece a los terceros que confían en caso de ocurrir suplantación de identidad por fallos en la operación del SVA.	
42	Información confidencial y/o privada	El PSVA debe mantener de manera confidencial la siguiente información: • Material comercialmente reservado de los PSCs, de los suscriptores de la empresa y de los 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.	
43	Información no privada	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.	
44	Derechos de Propiedad intelectual	De ser aplicable, el SVA debe declarar cláusulas contractuales de respecto de obligaciones y derechos relacionados a la propiedad intelectual.	
45	Notificaciones y comunicaciones entre participantes	El PSVA debe declarar los mecanismos de comunicación con sus clientes, en orden de realizar comunicaciones con valor legal.	
46	Conformidad con la Ley aplicable	El PSVA debe declarar la ley aplicable que debe ser cumplida por los participantes.	
47	Exención de garantías	En caso de existir, el PSVA debe declarar los casos de exención de garantías aplicables	
48	Indemnizaciones	En caso de existir, el PSVA debe declarar las indemnizaciones aplicables	
49	Fuerza mayor	En caso de existir, el PSVA debe declarar en algún documento normativo, las cláusulas de fuerza mayor que sean aplicables.	

3.2. SISTEMAS DE INTERMEDIACIÓN DIGITAL COMO SERVICIO

Los Sistemas de Intermediación Digital – Servicio son servicios web que permiten la transmisión y almacenamiento de información, garantizando el no repudio, confidencialidad e integridad de las transacciones a través del uso de componentes de firma digital, autenticación y canales seguros.

Una característica importante de esta SVA, es que se trata de servicios, por lo que se asume que se realiza un almacenamiento de datos, y puede involucrar la gestión de claves privadas de servidor.

Los SVA tipo Servicios de intermediación digital deben ser evaluados respecto del cumplimiento de los requerimientos descritos en la sección 8 y anexo I del presente documento.

3.2.1. Definición de Responsabilidades

Responsabilidades			
Explicación preliminar: Se deben definir las responsabilidades de las partes.			
No	Requerimiento		Detalle
1	Responsabilidades y obligaciones del PSVA	El PSVA deberá definir sus responsabilidades en relación con los usuarios de los sistemas del PSVA	
2	Responsabilidades y obligaciones del suscriptor	El PSVA deberá definir las responsabilidades de los suscriptores, usuarios de los sistemas de intermediación Digital como Producto	
3	Responsabilidades de los Terceros que confían	El PSVA deberá definir las responsabilidades de los terceros que confían, incluyendo:	

		• Verificar la validez de los certificados digitales de los documentos o información procesada por los sistemas de intermediación electrónica • Tomar en cuenta cualquier limitación en el uso de los sistemas considerados en la DPSVA • Tomar en cuenta cualquier otra precaución prescrita en los acuerdos u otra parte.	
4	Limitaciones de Responsabilidad	La TSA puede declarar o limitar cualquier responsabilidad excepto aquellas que sean estipuladas en la regulación vigente.	
5	Resolución de disputas	El PSVA debe establecer procedimientos para la resolución de disputas con sus clientes, indicando los datos de contacto o dirección a donde pueden dirigirse los reclamos.	

3.2.2. Gestión del ciclo de vida de las claves

Gestión del ciclo de vida de las claves			
Explicación preliminar: El PSVA debe proteger la clave privada que emplea para realizar firmas de sistemas automatizados a fin de evitar su compromiso.			
No	Requerimiento		Detalle
6	Generación de las claves	a) La Generación de las claves de firma del sistema automatizado deberá ser realizada en un ambiente asegurado físicamente, por personal que ocupa roles de confianza, bajo al menos el control de acceso de dos personas. El personal autorizado para realizar estas funciones debe estar limitado para realizar esta tarea conforme a los procedimientos del SVA. b) La generación de la clave de firma del sistema automatizado deberá ser realizada en un módulo criptográfico que: • Cumpla con los requerimientos FIPS 140-2 o • Cumpla los requerimientos identificados en el	Ejemplos de evidencias que deben ser requeridas: • Acta y procedimiento de generación u otro documento donde se especifican las condiciones técnicas y procedimientos vinculados a la generación de la clave, así como la identificación del personal de confianza encargado y su nombramiento • Documento donde se identifican los módulos criptográficos empleados y la evidencia de las certificaciones de seguridad correspondientes • Documentación o evidencia donde se especifiquen el algoritmo de generación de las claves, el tamaño de la clave y los algoritmos de firma, los cuales deben

		CEN Workshop Agreement 14167-2 (CWA 14167-2) c) El algoritmo de generación, la longitud de la clave firma y el algoritmo de firma usado para firmar los sellos de tiempo deberán ser reconocidos por la IOFE.	ser reconocidos por la IOFE • Documento donde se especifiquen los roles de confianza participantes, las responsabilidades y su debida asignación • Inspección visual del ambiente físico seguro donde se genera la clave
7	Protección de la clave privada	El PSVA debe asegurar que la clave privada de firma permanece confidencial y que se mantiene su integridad d) La clave de firma del sistema automatizado deberá ser protegida en un módulo criptográfico que: • Cumpla con los requerimientos FIPS 140-2 o • Cumpla los requerimientos identificados en el CEN Workshop Agreement 14167-2 (CWA 14167-2) e) Si se realiza un respaldo de la clave de firma, esta deberá ser copiada, almacenada y recuperada sólo por personal que ocupa roles de confianza, usando al menos el control de acceso de	Ejemplos de evidencias que deben ser requeridas: • Acta y procedimiento de protección para el almacenamiento de las copias de respaldo fuera del módulo criptográfico • Inspección visual del módulo criptográfico que está interconectado en el sistema de producción de los sellos de tiempo.

		dos personas. El personal autorizado para realizar estas funciones debe estar limitado para realizar esta tarea conforme a los procedimientos del SVA. f) Cualquier copia de la clave deberá ser protegida por la clave secreta del módulo criptográfico antes de ser almacenada fuera del dispositivo	
8	Distribución de la clave publica	La clave pública de firma debe ser disponible para los terceros que confían en un certificado de clave pública. El certificado puede ser emitido por la misma entidad que opera el SVA o por otra EC reconocida por la IOFE. El certificado debe ser emitido por una EC bajo una política que provea un nivel de seguridad equivalente o superior a la DPSVA. Este certificado deberá ser reconocido por la IOFE	Ejemplos de evidencias: • Procedimiento de distribución de la clave pública • Certificado digital que contiene la clave pública • Certificación que ampara la seguridad del certificado digital
9	Re-emisión de la clave	El tiempo de vigencia del certificado no debe ser mayor que el periodo de vigencia de los algoritmos y tamaños de claves, conforme al reconocimiento de la IOFE.	Ejemplos de evidencias: • Documentación donde se especifiquen las características técnicas referidas a la re-emisión de la clave

10	Término del ciclo de vida de la clave privada	El PSVA debe asegurar que las claves privadas no son usadas luego de expirado su ciclo de vida: d) Se deben establecer procedimientos técnicos u operacionales para asegurar que son generadas y utilizadas nuevas claves e) La clave privada de firma, o cualquier parte de la clave debe ser destruida de tal modo que no pueda ser recuperada f) El sistema de generación de sellos de tiempos debe rechazar cualquier intento de emitir sellos de tiempo si la clave privada de firma ha expirado o se encuentra revocada.	Ejemplos de evidencias: • Procedimiento de gestión de la clave luego de su expiración o revocación: • Emisión de una nueva clave • Destrucción de la clave expirada o revocada, incluyendo cualquier copia • Impedimento de emisión de sello de tiempo

3.2.3. Ciclo de vida del módulo criptográfico

Ciclo de vida del módulo criptográfico		
Explicación preliminar: El PSVA debe proteger el módulo criptográfico donde se almacena su clave privada, a fin de evitar su compromiso.		
No	Requerimiento	Detalle

11	Gestión del ciclo de vida del módulo criptográfico	a) El hardware del módulo criptográfico no debe ser manipulado durante su transporte b) El hardware del módulo criptográfico no debe ser manipulado durante su almacenamiento c) La instalación, activación y duplicación de la clave de firma en el hardware del módulo criptográfico deberá ser realizado solo por personal que ocupa roles de confianza, usando al menos un control de acceso de dos personas en un ambiente físico seguro. d) El hardware de firma de sellos de tiempo funciona correctamente e) Las claves de firma que son almacenadas en un módulo criptográfico son borradas antes de que el dispositivo sea retirado	Ejemplos de evidencias • Procedimiento de gestión del módulo criptográfico Pruebas de aseguramiento de correcto funcionamiento del equipo Registros de borrado de claves privadas antes de que el equipo sea desechado

3.2.4. Autenticación

Autenticación			
Explicación preliminar: En caso que los sistemas contemplen funciones de validación de identidad de sus usuarios mediante un certificado digital, deberán verificar la validez del mismo antes de autorizar su acceso.			
No	Requerimiento		Detalle
12	Validación de la confiabilidad de la raíz	El sistema deberá verificar que el certificado corresponde a una Entidad de Certificación reconocida por la IOFE, de no ser exitosa la verificación, el sistema no debe permitir el acceso.	
13	Validación del estado de revocación	El sistema deberá verificar que tanto el certificado del usuario final, así como los certificados que componen la cadena de certificación no se encuentran revocados. Esta verificación puede ser mediante los mecanismos CRL u OCSP. En caso de ser CRL, se deberá verificar la vigencia y autenticidad de la CRL.	La autenticidad de la CRL se verifica mediante la verificación de la firma, buscando que haya sido realizada por la EC que emitió la CRL.
14	Validación del estado de vigencia	El sistema deberá verificar que tanto el certificado del usuario final, así como los certificados que componen la cadena de certificación se encuentran vigentes, es decir, que su periodo de vida no ha expirado.	

15	Validación del propósito	El sistema deberá verificar que el certificado del usuario final tiene como propósito autenticación, conforme a la RFC 5280.	

3.2.5. Cifrado

Cifrado			
Explicación preliminar: En caso que los sistemas realicen funciones de cifrado con certificados digitales, se deberá proteger la clave privada empleada en los procesos de cifrado			
No	Requerimiento		Detalle
16	Protección de la clave privada	Al momento de descifrar la información, el sistema no deberá copiar la clave privada sin cifrar fuera del módulo criptográfico. La clave privada siempre debe mantenerse dentro del módulo criptográfico.	
17	Validación de la confiabilidad de la raíz	El sistema deberá verificar que el certificado corresponde a una Entidad de Certificación reconocida por la IOFE, de no ser exitosa la verificación, el sistema no debe permitir el acceso.	
18	Validación del estado de revocación	El sistema deberá verificar que tanto el certificado del usuario final, así como los certificados que componen la cadena de certificación no se encuentran revocados.	La autenticidad de la CRL se verifica mediante la verificación de la firma, buscando que haya sido realizada por la EC que emitió la CRL.

		Esta verificación puede ser mediante los mecanismos CRL u OCSP. En caso de ser CRL, se deberá verificar la vigencia y autenticidad de la CRL.	
19	Validación del estado de vigencia	El sistema deberá verificar que tanto el certificado del usuario final, así como los certificados que componen la cadena de certificación se encuentran vigentes, es decir, que su periodo de vida no ha expirado.	
20	Validación del propósito	El sistema deberá verificar que el certificado del usuario final tiene como propósito de cifrado o cifrado de clave, conforme a la RFC 5280.	

3.2.6. Canales SSL

Canales SSL			
Explicación preliminar: En caso que los sistemas implementen canales seguros SSL			
No	Requerimiento		Detalle
21	Protección de la clave privada	Al momento de descifrar la información, el sistema no deberá copiar la clave privada sin cifrar fuera del módulo criptográfico. La clave privada siempre debe mantenerse dentro del módulo criptográfico.	

22	Validación de la confiabilidad de la raíz	El sistema deberá verificar que el certificado corresponde a una Entidad de Certificación reconocida por la IOFE, de no ser exitosa la verificación, el sistema no debe permitir el acceso.	
23	Validación del estado de revocación	El sistema deberá verificar que tanto el certificado del usuario final, así como los certificados que componen la cadena de certificación no se encuentran revocados. Esta verificación puede ser mediante los mecanismos CRL u OCSP. En caso de ser CRL, se deberá verificar la vigencia y autenticidad de la CRL.	La autenticidad de la CRL se verifica mediante la verificación de la firma, buscando que haya sido realizada por la EC que emitió la CRL.
24	Validación del estado de vigencia	El sistema deberá verificar que tanto el certificado del usuario final, así como los certificados que componen la cadena de certificación se encuentran vigentes, es decir, que su periodo de vida no ha expirado.	
25	Validación del propósito	El sistema deberá verificar que el certificado del usuario final tiene como propósito de cifrado de clave, conforme a la RFC 5280.	

3.2.7. Petición de sellos de tiempo

Petición de sellos de tiempo			
Explicación preliminar: En caso que los sistemas realicen peticiones de sellos de tiempo, deben cumplir requisitos que garanticen su confiabilidad			
No	Requerimiento		Detalle
26	Formato de petición	El formato de petición debe ser conforme a la RFC 3161.	
27	Validación de la confiabilidad de la raíz	El sistema deberá verificar que el certificado con el que se firma el sello de tiempo corresponde a una Entidad de Certificación reconocida por la IOFE.	
28	Validación del estado de revocación	El sistema deberá verificar que el certificado con el que se firman los sellos de tiempo no se encuentra revocado.	
29	Validación del estado de vigencia	El sistema deberá verificar que el certificado con el que se firman los sellos de tiempo no se encuentra expirado.	
30	Validación de la firma	El sistema deberá verificar la firma del sello de tiempo para corroborar que los datos son íntegros	

3.2.8. Gestión de la seguridad

Gestión de la seguridad			
Explicación preliminar: El PSVA debe implementar los controles necesarios para asegurar la información en sus operaciones			
No	Requerimiento		Detalle
31	Organización de la seguridad de la información	Debe existir un responsable de organizar y dirigir la seguridad de la información	
32	Política de seguridad de la información	Se debe implementar y establecer una Política de seguridad cuyo alcance cubra todas las operaciones críticas del SVA El PSVA deberá asegurar la publicación de esta Política y comunicación a todos los empleados que participan de las operaciones del SVA.	
33	Seguridad en el trato con terceros	• La seguridad debe ser mantenida cuando las funciones son tercerizadas a otra organización o entidad. El PSVA es responsable de los servicios que brinda, incluyendo los que son realizados por terceros proveedores • Las responsabilidades de terceros deben ser	

		definidas y deben hacerse arreglos para asegurar que los terceros cumplen todos los controles requeridos • El PSVA deberá mantener la responsabilidad de declarar las prácticas relevantes de tercerización a todas las partes interesadas	
34	Seguridad del personal	j) El PSVA deberá emplear personal que posea conocimiento especializado, experiencia y calificaciones necesarias para ofrecer los servicios, de acuerdo a las funciones que debe cumplir cada rol k) Los roles y responsabilidades referidas al cumplimiento de la Política de Seguridad, deben ser documentados en las descripciones de las funciones de cada rol. Los roles de confianza, de los cuales dependen las operaciones del SVA deberán ser identificados. l) Las funciones del personal del SVA	

		(temporal y permanente) deberán definidas considerando los criterios de separación de derechos y mínimo privilegio m) El personal deberá ejecutar sus funciones y procedimientos en función de los procedimientos y la Política de Seguridad. n) El personal gerencial debe tener conocimiento de las tecnologías relacionadas a los servicios del SVA, como firma digital, gestión de certificados digitales, sello de tiempo, mecanismos de sincronización de relojes con la UTC, conocimientos de los procedimientos y responsabilidades de seguridad para la gestión de personal, experiencia en seguridad de la información y evaluación de riesgos. o) Todo el personal en roles de confianza debe ser libre de conflicto de interés que pueda perjudicar la imparcialidad de las operaciones del SVA	

		p) Los roles de confianza deben incluir las siguientes responsabilidades: • Oficiales de seguridad: Responsables de administrar la implementación de las prácticas de seguridad • Administradores de sistemas: Autorizados a instalar, configurar y mantener la integridad de los sistemas del SVA • Operadores de sistemas: Responsable de operar la integridad de los sistemas en el día a día. Autorizados para ejecutar sistemas de respaldo y recuperación. • Auditores de sistemas: Autorizados a ver archivos y logs de los sistemas del SVA q) El personal debe ser formalmente asignado a cumplir los roles de confianza, por parte del responsable gerencial de la seguridad	

		r) El PSVA no deberá asignar en roles de confianza o administración a cualquier persona que es conocida por tener una participación en un crimen serio u otra ofensa la cual afecta su idoneidad para su puesto. El personal no deberá tener acceso a funciones de confianza hasta completar todas las verificaciones necesarias.	
35	Seguridad física y del entorno	e) Los medios de administración de los sistemas del SVA deberán ser operados en un ambiente protegido con controles físicos de acceso para proteger de acceso no autorizado a los sistemas y datos f) Se deben definir perímetros de seguridad que protejan las operaciones y sistemas críticos del SVA. Las partes compartidas con otras organizaciones deberán ser afuera de este perímetro. g) Controles de seguridad física y ambiental deben ser implementados para proteger los medios que alojan los recursos informáticos, los recursos informáticos, y los medios usados para soportar su operación.	Ejemplos de evidencias: Inspección visual de la implementación de: • Acceso físico limitado apropiadamente a individuos autorizados • Operación de medios de procesamiento desde ambiente con protección física • Controles contra pérdida, daños o compromiso de los activos de información, así como interrupción de las actividades del negocio • Controles contra compromiso o robo de información y sus medios de procesamiento • Controles de seguridad ambientales (controles contra incendio, regulación de humedad, temperatura)

		Estos deben incluir: protección de acceso físico, protección contra desastres naturales, detección y protección contra incendios, contingencia en cortes de energías y comunicaciones, colapso de la estructura, aniego, protección contra robo, ruptura, recuperación en caso de desastres, conforme a los resultados del análisis de riesgos. Se deben implementar controles que impidan el retiro no autorizado de equipos, información, medios de almacenamiento, software relativo a los servicios críticos del SVA.	
36	Gestión de operaciones	g) La integridad de los componentes informáticos y la información deben ser protegidos contra virus, software malicioso o no autorizado. h) Se deben implementar y ejecutar procedimientos de reporte y respuestas a incidentes de seguridad y mal funcionamiento de las operaciones del SVA i) Los medios de almacenamiento usados en los sistemas críticos del SVA deben ser protegidos contra	Gestión de operaciones

		modificación o acceso no autorizados j) Se deben establecer procedimientos para todos los roles de confianza y administrativos que impactan en la provisión de servicios del SVA. k) Se deben implementar procedimientos para asegurar la adecuada planificación de activos y nuevos sistemas a fin de evitar incompatibilidades con otros sistemas y vulnerabilidades de seguridad l) La limpieza de los ambientes debe ser adecuada para no dañar los equipos, y el personal debe ser supervisado para evitar robos de medios de almacenamiento e información	
37	Manejo de medios y seguridad	Todos los medios deben ser manejados de manera segura conforme a la clasificación de activos. Los medios de almacenamiento que contienen datos sensibles deben ser eliminados de manera segura cuando ya no sean requeridos.	
38	Planificación del sistema	Las demandas de capacidad de los sistemas deben ser monitoreadas y deben realizarse	

		proyecciones de la demanda futura a fin de asegurar la disponibilidad de los sistemas de procesamiento y almacenamiento.	
39	Reporte y respuesta a incidentes	El PSVA debe actuar de manera oportuna y coordinada para responder de manera rápida a los incidentes y limitar el impacto de los vacíos de seguridad. Todos los incidentes deben ser reportados tan pronto como sea posible.	Ejemplos de evidencias: Reportes de incidentes, informes de seguimiento y solución Estadísticas de incidentes reportados y atendidos
40	Seguridad en redes	• Debe definirse una política de acceso en redes • Las redes deben ser protegidas de acceso no autorizado, • Se debe separar la zona de constante acceso con la red interna de procesamiento y almacenamiento de información crítica. De acuerdo a los diferentes niveles de seguridad, deben separarse las redes de datos de los sistemas de procesamiento central del SVA • El acceso a dominios de redes internas del SVA deben ser protegidos de acceso o autorizado incluyendo a suscriptores y terceros que confían. Los	

		firewalls deben ser configurados para prevenir todos los protocolos y accesos no requeridos para la operación del SVA Deben implementarse sistemas de detección de intrusos para prevenir accesos de código malicioso o no autorizado	
41	Monitoreo	• La continuidad y seguridad de las operaciones debe ser monitoreada. • Los registros de auditoría y los reportes de eventos sobre errores y advertencias en el funcionamiento de los sistemas del SVA deben ser monitoreados Medios de monitoreo y alarmas deben ser implementados para detectar, registrar y actuar oportunamente sobre accesos no autorizados o intentos irregulares de acceso a recursos.	
42	Intercambio de datos y software	Se debe evaluar las vulnerabilidades y riesgos de seguridad relacionados al intercambio de datos y software, y estos deben ser manejados de manera apropiada de acuerdo a su impacto sobre las operaciones del SVA	

43	Gestión de accesos a los sistemas	En caso que el sistema se encuentre integrado a un sistema de gestión de usuarios, este deberá cumplir lo siguiente: • Permitir la asignación de cuentas de usuario para controlar los accesos a los sistemas, permitir la modificación o remoción oportuna de accesos. • Diferenciar las cuentas de administración de las cuentas de usuario. • El sistema debe permitir controlar al personal respecto de las acciones críticas que realiza en los sistemas del SVA, generando registros de auditoria.	
44	Archivo	La información crítica y sensible, que es archivada debe ser protegida contra daño ambiental o intencional, así como acceso de lectura y modificación no autorizados.	Ejemplo de evidencia: Procedimiento de gestión del archivo.
45	Desarrollo y mantenimiento de sistemas confiables	Se debe realizar un análisis de los requerimientos de seguridad que deben ser cubiertos en las etapas de diseño y especificación de los proyectos de desarrollo de sistemas del SVA, para asegurar que dichos	Ejemplos de evidencias: Documento donde se establece el análisis de requerimientos de seguridad en la etapa de diseño y especificación de requerimientos de todo proyecto de desarrollo

		requerimientos son considerados en los sistemas críticos	realizado por o en nombre del PSVA
46	Control de cambios	Se debe implementar procedimientos de control de cambios para poner en producción modificaciones o parches de emergencia de aplicaciones críticas de software del SVA, a fin de evitar posteriores fallas o incompatibilidad con otros sistemas.	Ejemplo de evidencias: Procedimientos de control de cambios

3.2.9. Término de la organización que administra el SVA

Término del PSVA			
Explicación preliminar: El PSVA debe adoptar las medidas necesarias para que su finalización no afecte de manera significativa a los suscriptores y terceros que confían.			
No	Requerimiento		Detalle
47	Preparación antes del término	a) El PSVA debe poner a disponibilidad de los suscriptores y terceros que confían la información concerniente a su terminación b) El PSVA deberá terminar con las autorizaciones de todos los subcontratistas que actúan en nombre del PSVA, c) Asegurar el cumplimiento o compensación por los servicios comprometidos de soporte o garantía	Acuerdos para cubrir los costos mínimos, en caso se declare la quiebra u otras razones que le impidan cubrir los costos

3.2.10. Registros de auditoría

Registros de auditoría			
Explicación preliminar: El sistema debe permitir registrar los eventos críticos			
No	Requerimiento		Detalle
48	Eventos registrados	El PSVA debe declarar los tipos de eventos y datos que serán registrados. Los eventos que deben ser registrados deben ser relacionados a las transacciones de autenticación y generación de firma digital.	
49	Protección de los registros	Los eventos deben ser registrados en un modo que ellos no puedan ser borrados o destruidos dentro del periodo de tiempo que son requeridos como evidencia (excepto si son transferidos a medios de almacenamiento de largo plazo).	
50	Eventos significativos	Deben ser registradas las solicitudes o transacciones de firma digital, autenticación o cifrado	

3.2.11. Auditoria

Auditoría			
Explicación preliminar: El PSVA debe ser auditada anualmente por la AAC, respecto de la correcta operación de los servicios de registro.			
No	Requerimiento		Detalle
51	Auditoría de registros	Los registros deben ser revisados como parte de la auditoría de la AAC, de manera anual.	
52	Auditoría del archivo	El archivo debe ser revisado como parte de la auditoría de la AAC, de manera anual.	
53	Auditoría de los procedimientos y controles	Los procedimientos y controles implementados deben ser auditados por la AAC de manera anual.	
54	Auditor	El auditor debe: • Ser autorizado por la AAC. • Ser independiente del PSVA, y no haber realizado trabajos para ella dentro de los 2 años anteriores a la ejecución de la auditoría.	

3.2.12. Certificados de autenticación

Certificados de autenticación			
Explicación preliminar: Conforme al D.S. 052-2008-PCM, el PSVA puede emitir certificados de autenticación para ser utilizados por sus usuarios en la operación de los servicios de valor añadido.			
No	Requerimiento		Detalle
55	Certificados	Para emitir los certificados, la PSVA debe utilizar los servicios de una EC acreditada o reconocida por la IOFE	
56	Solicitud de emisión, revocación, re-emisión, suspensión o modificación	Las solicitudes de emisión, revocación, re-emisión, suspensión o modificación deben ser realizadas a través de una Entidad de Registro o de un Canal Seguro de Registro y Distribución de Certificados Digitales acreditados por la AAC.	
57	Gestión de los certificados digitales de persona jurídica	Al retirarse una persona del campo de usuarios de los servicios de valor añadido, su certificado digital debe ser revocado o suspendido en función del periodo de tiempo definido para su retiro. Ninguna persona jurídica podrá guardar claves privadas de sus suscriptores, a menos que pueda garantizar que en ningún	

		momento la clave privada podrá ser usada sin la autorización exclusiva del suscriptor. La persona jurídica no podrá guardar copias de las claves privadas de los suscriptores en formatos .PFX o PKCS#7	

3.2.13. Aspectos legales de la Operación SVA

Aspectos legales de la operación del SVA			
Explicación preliminar:			
No	Requerimiento		Detalle
58	Políticas de reembolso	El PSVA debe declarar, si fuera aplicable, políticas de reembolso, incluyendo los siguientes casos,	
59	Cobertura de seguro de responsabilidad civil	El monto mínimo de la póliza es de $ 35 000. 00 dólares americanos. El PSVA debe publicar las garantías financieras que ofrece a los terceros que confían en caso de ocurrir suplantación de identidad por fallos en la operación del SVA.	

60	Información confidencial y/o privada	El PSVA debe mantener de manera confidencial la siguiente información: • Material comercialmente reservado de los PSCs, de los suscriptores de la empresa y de los 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.	
61	Información no privada	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.	
62	Derechos de Propiedad intelectual	De ser aplicable, el PSVA debe declarar cláusulas contractuales de respecto de obligaciones y derechos relacionados a la propiedad intelectual.	
63	Notificaciones y comunicaciones entre participantes	El PSVA debe declarar los mecanismos de comunicación con sus clientes, en orden de realizar comunicaciones con valor legal.	
64	Procedimiento de resolución de disputas	El PSVA debe establecer contractualmente y en la DPSVA los procedimientos para solucionar disputas con sus clientes	

64	Conformidad con la Ley aplicable	El PSVA debe declarar la ley aplicable que debe ser cumplida por los participantes.	
65	Exención de garantías	En caso de existir, el PSVA debe declarar los casos de exención de garantías aplicables	
66	Indemnizaciones	En caso de existir, el PSVA debe declarar las indemnizaciones aplicables	
67	Fuerza mayor	En caso de existir, el PSVA debe declarar en algún documento normativo, las cláusulas de fuerza mayor que sean aplicables.	