AUTORIDAD DE INTERMEDIACIÓN ELECTRÓNICA	Fecha: 20/02/2017
	Versión: 2

MAPEO ENTRE LA DPSVA Y EL MARCO DE LA POLÍTICA DE PRESTACIÓN DE SERVICIOS DE VALOR AÑADIDO

SISTEMA DE INTERMEDIACIÓN DIGITAL

info@saeta.pe • www.saeta.pe
General Vidal 921 - Breña • (511) 633 - 7824 / 333 - 2212

Elaborado	Fecha de Elaboración	Versión
José Junior Damian Tirado (Jefe de Aplicaciones y Desarrollo)	20/02/2017	2

Revisado	Fecha de Revisión	Versión
Jesús Ojeda (Oficial de Seguridad)	02/03/2017	2

INTRODUCCIÓN

Cualquier Sistema de Redes de Computadoras ya sea in-house o en la nube (ordenadores, periféricos, nodos y accesorios) están expuestos a riesgo y puede ser fuente de problemas. El Hardware, el Software están expuestos a diversos Factores de Riesgo Humano y Físicos. Estos problemas menores y mayores sirven para retroalimentar nuestros procedimientos y planes de seguridad en la información. Pueden originarse pérdidas catastróficas a partir de fallos de componentes críticos (el disco duro), bien por grandes desastres (incendios, terremotos, sabotaje, etc.) o por fallas técnicas (errores humanos, virus informático, etc.) que producen daño físico irreparable. Por lo anterior es importante contar con un Plan de contingencia adecuado de forma que ayude a la Entidad a recobrar rápidamente el control y capacidades para procesar la información y restablecer la marcha normal del negocio.

La protección de la información vital de una entidad ante la posible pérdida, destrucción, robo y otras amenazas, es abarcar la preparación e implementación de un completo Plan de Contingencia de TI.

Para elaborar esta declaración de prácticas de Servicio Añadido de SOLUCIONES APLICADAS EN TECNOLOGÍA AVANZADA se tiene en cuenta la información como uno de los activos más importantes de la Organización, además que la infraestructura informática está conformada por el hardware, software y elementos complementarios que soportan la información o datos críticos para la función de la Entidad, siendo el principal proceso de negocio de la organización, la transformación digital. Y con ello la herramienta de intermediación electrónica, llamada Plussigner, que tiene como objetivo brindar soluciones con la capacidad de poder certificar documentos y procesos que conllevan a la transformación digital de cualquier organización de índole ya sea pública o privada.

1. INTRODUCCIÓN

Cualquier Sistema de Redes de Computadoras ya sea in-house o en la nube (ordenadores, periféricos, nodos y accesorios) están expuestos a riesgo y puede ser fuente de problemas. El Hardware, el Software están expuestos a diversos Factores de Riesgo Humano y Físicos. Estos problemas menores y mayores sirven para retroalimentar nuestros procedimientos y planes de seguridad en la información. Pueden originarse pérdidas catastróficas a partir de fallos de componentes críticos (el disco duro), bien por grandes desastres (incendios, terremotos, sabotaje, etc.) o por fallas técnicas (errores humanos, virus informático, etc.) que producen daño físico irreparable. Por lo anterior es importante contar con un Plan de contingencia adecuado de forma que ayude a la Entidad a recobrar rápidamente el control y capacidades para procesar la información y restablecer la marcha normal del negocio.

La protección de la información vital de una entidad ante la posible pérdida, destrucción, robo y otras amenazas, es abarcar la preparación e implementación de un completo Plan de Contingencia de TI.

Para elaborar el mapeo entre el Marco de la Política de Prestación de Servicios de Valor Añadido y el DPSVA de SOLUCIONES APLICADAS EN TECNOLOGÍA AVANZADA se tiene en cuenta la información como uno de los activos más importantes de la Organización, además que la infraestructura informática está conformada por el hardware, software y elementos complementarios que soportan la información o datos críticos para la función de la Entidad, siendo el principal proceso de negocio de la organización la transformación digital. Este Plan implica realizar un análisis de los posibles riesgos a los cuales pueden estar expuestos nuestros equipos de cómputo y sistemas de información, de forma que se puedan aplicar medidas de seguridad oportunas y así afrontar contingencias y desastres de diversos tipos.

Los procedimientos relevantes a la infraestructura informática, son aquellas tareas que el personal realiza frecuentemente al interactuar con la plataforma informática (entrada de datos, generación de reportes, consultas, etc.).El Plan de Contingencia está orientado a establecer un adecuado sistema de seguridad física y lógica en previsión de desastres, de tal manera de establecer medidas destinadas a salvaguardar la información contra los daños producidos por hechos naturales o por el hombre.

2. OBJETIVO DEL DOCUMENTO

Este documento tiene como objeto el mapeo entre la DPSVA y el Marco de la Política de Prestación de Servicios de Valor Añadido, acorde al reglamento específico de la SVA, ubicado en el anexo 7 de la documentación de la guía de acreditación para prestadoras de Servicios de Valor Añadido.

3. OBJETO DE LA ACREDITACIÓN

El alcance de la acreditación del Sistema de Intermediación Digital de PLUSSIGNER en el marco del cumplimiento de los requerimientos de la “Guía de Acreditación de Prestadores de Servicios de Valor Añadido (SVA)” establecida por el INDECOPI, comprende la representación de las siguientes plataformas:

Plussigner, es una plataforma de intermediación electrónica que tiene la capacidad de captar y administrar documentos electrónicos, garantizando confidencialidad, disponibilidad y autenticidad, teniendo las siguientes características principales:

- Trazabilidad de Documentos Electrónicos: Desde que fue recibido por la plataforma hasta la entrega de los correos electrónicos a los involucrados de la notificación.
- Transferencia de Documentos Electrónicos: Garantizando el traslado de la información bajo medidas de confidencialidad, disponibilidad y autenticidad que garantizan las comunicaciones y transferencia de documentos de forma segura y rápida.
- Firma y Sello de Tiempo de Documentos Electrónicos: Los documentos de Firma pasan por un Módulo de Firma acreditado como es SSigner que brinda el servicio de certificación digital de los documentos electrónicos, otorgando adicionalmente el Sello de Tiempo.
- Envío de correos certificados a través de firma electrónica: Los correos electrónicos son firmados digitalmente a través de plussigner para garantizar la autenticidad y seguridad de la notificación electrónica.
- Así como la custodia de Documentos Electrónicos: Este resguardo va conforme a lo establecido y con mecanismos que garanticen la confidencialidad, disponibilidad y la disponibilidad de estos documentos.

Soluciones Aplicadas en Tecnología Avanzada S.A.C. es responsable de exigir el cumplimiento de los requisitos establecidos por la Autoridad Administrativa Competente de la IOFE a sus proveedores y es responsable ante sus clientes de la calidad y seguridad de los servicios brindados.

Los proveedores por si mismos no se encuentran amparados por la presente acreditación, sino solamente a través del control de calidad y seguridad que exige Soluciones Aplicadas en Tecnología Avanzada S.A.C. a sus proveedores. Es necesario tener en cuenta que los proveedores de este tipo de servicios pueden ser con proveedores en la nube privada, híbrida y pública o en equipos locales que cumplan con las características técnicas que requiera la plataforma Plussigner.

4. MAPEO ENTRE DPSVA Y MPPSVA

ESQUEMA		MPPSVA	DPSVA	Observaciones / Comentarios
INTRODUCCION	INTRODUCCION	Se debe presentar toda la documentación requerida en la Guía de Acreditación de Prestadores de Servicio de Valor Añadido (SVA) y sus anexos, además deberá seguir los procedimientos respectivos de acuerdo a la ley vigente y al Reglamento General de Acreditación Prestadores de Servicios de Certificación Digital -ver anexo 7- así como el Reglamento Específico de Acreditación Prestadores de Servicios de Valor Añadido (SVA).	Se tiene un documento DPSVA que contiene los ítems que solicita INDECOPI.	Para la Intermediación de Plussigner se aplica como servicio y también otorgado al cliente en sus instalaciones.
		Para la acreditación como SVA que realiza procedimientos con firma digital de usuarios finales, se requiere el empleo de un aplicativo (software) que se encuentre acreditado conforme a lo establecido en el Reglamento de acreditación de aplicaciones (SW) de clave pública (PKI).	Se cuenta con un software de Firma Digital llamado SSigner bajo resolución 102-2016/CFE-INDECOPI con fecha 20/10/2016	
PARTICIPANTES	2.1. Comunidad de Usuarios	La comunidad de usuarios se compone por aquellas personas naturales y jurídicas que utilizan los servicios de un SVA, los cuales cumplen los requerimientos especificados en las siguientes secciones de este documento.	Soluciones Aplicadas en Tecnología Avanzada S.A.C. brinda sus servicios de valor añadido a personas jurídicas del sector privado y gubernamental.	
	2.2. Tercero que confía (tercer usuario)	La comunidad de terceros que confían de un SVA puede ser más restringida que aquella establecida bajo el marco de la IOFE. La VAPS del SVA debe detallar los requerimientos que se deben cumplir para participar como tercero que confía dentro del ámbito de dicho SVA.	Los terceros que confían son todas aquellas personas naturales y jurídicas, incluyendo entidades de otras infraestructuras además de la IOFE, que requieren evaluar la validez de una transacción electrónica, un documento firmado o un certificado utilizado o generado en los servicios brindados por los servicios brindados por la plataforma PLUSSIGNER de Soluciones Aplicadas en Tecnología Avanzada S.A.C.	
SERVICIOS	3.1. Tipos de servicios	El SVA debe especificar en su VAPS o en otro documento relevante los tipos de servicios que	Esto se especifica en la sección “PLATAFORMA” del VAPS.	

		brindará y una descripción técnica general de cada servicio, garantizando el no compromiso del par de claves de firma y autenticación de sus usuarios.		
	3.2. Uso apropiado de los certificados de los usuarios finales en los servicios brindados.	Los SVAs deben establecer en su VAPS u otro documento relevante, las limitaciones técnicas y normativas del uso de los certificados en los servicios brindados, estas limitaciones deben estar relacionadas con la seguridad y el no compromiso de las claves de firma y autenticación. En particular, debe establecerse un uso apropiado de los certificados para las transacciones de comercio y/o gobierno electrónico.	Esta sección se especifica en la arquitectura de la solución de Intermediación Electrónica Plussigner.	
ADMINISTRACIÓN DE POLÍTICAS	4.1. Organización que administra los documentos de VAPS	Los detalles de contacto respecto a SVAs deben ser registrados en las VAPS de dichas entidades. Se debe incluir el nombre y la dirección de envío de la organización Que es responsable del diseño, registro, mantenimiento, y actualización de esta VAPS.	La empresa es SOLUCIONES APLICADAS EN TECNOLOGÍA AVANZADA S.A.C. (SAETA)	
	4.2. Persona de contacto	Los detalles de contacto respecto a SVAs deben ser registrados en las VAPS de dichas entidades. Se debe incluir el nombre y la dirección de envío de la organización que es responsable del diseño, registro, mantenimiento, y actualización de esta VAPS.	La persona de contacto: Nombre: José Junior Damian Tirado Puesto: Sub Gerente General Teléfono: +511979668777 Correo: jose.damian@saeta.pe	
PUBLICACIÓN	5.1. Tiempo o frecuencia de la publicación	Las modificaciones relativas a la VAPS u otra documentación de los SVAs, deben ser publicadas tan pronto como razonablemente sea posible, debiendo tener cuidado de cumplir con los requisitos que fueren necesarios para la aprobación de dichas modificaciones.	Normalmente las publicaciones serán comunicadas y aprobadas por INDECOPI, y su tiempo de cambio, dependerá de la prioridad que dé la IOFE para tal fin. Por temas de buenas prácticas se considerará con mínimo un plazo de un año	
	5.2. Controles de acceso a las publicaciones y bases de datos	Dentro de su comunidad de usuarios, el SVA no debe limitar el acceso de lectura a las informaciones establecidas en su VAPS y demás documentos relevantes (contemplados en la sección 5), pero debe restringir su modificación sólo a personal autorizado.	Estas políticas de uso son restringidas dependiendo el privilegio que tengan en la organización, así como la responsabilidad que tenga con respecto a la SVA.	

REQUISITOS OPERACIONALES DEL CICLO DE VIDA DE LOS CERTIFICADOS Y SERVICIOS	6.1. Certificados de autenticación	Los SVAs podrán generar certificados de autenticación a los usuarios que los soliciten. Dichos certificados serán utilizados sólo en los casos en los que se requiera la autenticación del usuario para el control de acceso a domicilios electrónicos, correspondientes a los servicios vinculados a notificaciones electrónicas. Su uso fuera del servicio, en aplicaciones ajenas al SVA que lo emitió, no será reconocido por la IOFE.	No aplica	
	6.2. Actualización de los certificados en el sistema del SVA	En caso que el certificado de autenticación de un usuario haya expirado o haya sido revocado, el SVA debe requerir de dicho usuario obtener un nuevo certificado y proporcionar al SVA los datos necesarios para configurar su nuevo certificado en el SIE y gestionar el control de acceso a su domicilio electrónico.	No aplica	
	6.3. Solicitud del servicio	En la solicitud, los usuarios deberán especificar los detalles del certificado de autenticación que utilizarán dentro del servicio. Dichos detalles deben ser establecidos en la VAPS del SVA. El certificado podrá ser emitido por cualquier EC acreditada (en este caso podrá ser utilizado fuera del servicio del SVA) o por el mismo SVA.	No aplica	
	6.4. Requerimientos para la verificación de la revocación de certificados por el SVA	El sistema informático del SVA debe establecer la validez de un certificado al momento de la realización de cada transacción, y debe asumir las consecuencias de eventuales omisiones.	No aplica	
	6.5. Requerimientos para la verificación de la revocación de certificados por los terceros que confían	Los servicios brindados por el SVA deben permitir al tercero que confía verificar el estado de confiabilidad de un certificado, lo cual implica verificar lo siguiente: ○ La cadena de certificación o según sea el caso, la TSL. ○ La CRL o el Delta-CRL.	No aplica	
	6.6. Depósito de claves	No está permitido para el SVA el almacenamiento de ninguna de las claves privadas de los certificados digitales de sus usuarios.	No aplica	
CONTROLES DE	7.1. Controles	La ubicación y diseño del local debe prevenir, en	Estos controles se encuentran en la	

LAS INSTALACIONES, DE LA GESTION Y CONTROLES OPERACIONALES	Físicos	lo razonablemente posible, el daño por desastres naturales, como inundación, terremoto; así como desastres creados por el hombre, como incendios, disturbios civiles y otras formas de desastre.	Política de Seguridad de la Información. Haciendo énfasis que nuestra intermediación como servicio se encuentra en la NUBE de Amazon Web Services y OVH.	
	7.2. Controles Procesales - 7.2.1. Roles de confianza	Se deben definir los roles de confianza en las operaciones que se realizan en los SVAs.	Estos controles se encuentran en la Política de Seguridad de la Información. En el VAPS se hace referencia a la Política de Seguridad de la Información.	
	7.2. Controles Procesales - 7.2.2. Número de personas requeridas por labor	Se debe identificar las labores que requieren de más de una persona para su realización.	Estos controles se encuentran en la Política de Seguridad de la Información. En el VAPS se hace referencia a la Política de Seguridad de la Información.	
	7.2. Controles Procesales - 7.2.3. Identificación y autenticación para cada rol	Deben emplearse controles de acceso tanto físicos como lógicos para verificar la identidad y autorización correspondiente a cada función, antes de permitir el acceso a servidores y equipos que manejen información sensible.	Estos controles se encuentran en la Política de Seguridad de la Información. En el VAPS se hace referencia a la Política de Seguridad de la Información.	
	7.2. Controles Procesales - 7.2.4. Roles que requieren funciones por separado	Se deben definir los roles que requieren la separación de funciones para la operación de los SVAs.	Estos controles se encuentran en la Política de Seguridad de la Información. En el VAPS se hace referencia a la Política de Seguridad de la Información.	
	7.3. Controles de Personal -	Los SVAs deben establecer en su VAPS, los términos de confidencialidad y provisiones de no revelación que gobierna al mismo, de conformidad con la Norma Marco sobre Privacidad presentada en el anexo 5 de la Guía de Acreditación de SVA. Así como la legislación que rige a las transacciones que se realizan bajo el marco de la IOFE, la legislación relativa al régimen de los trabajadores y cualquier otra legislación relevante.	Estos controles se encuentran en la Política de Seguridad de la Información. En el VAPS se hace referencia a la Política de Seguridad de la Información.	
	7.3. Controles de Personal - 7.3.1. Cualidades y requisitos,	Los SVAs y deben establecer en su VAPS u otra documentación relevante las cualidades, experiencias y certificados que deben poseer su personal y contratistas.	Se encuentra en la memoria Descriptiva y organigrama estructural y funcional del SIE.	

	experiencia y certificados			
	7.3. Controles de Personal - 7.3.2. Procedimiento para verificación de antecedentes.	Se deben de establecer los procedimientos para la verificación de antecedentes pudiéndose determinar a la persona encargada de realizar dicha verificación.	Estos controles se encuentran en la Política de Seguridad de la Información. En el VAPS se hace referencia a la Política de Seguridad de la Información.	
	7.3. Controles de Personal - 7.3.3. Requisitos de capacitación	Todos los empleados de la organización (y cuando sea relevante los contratistas y terceros), deben recibir las capacitaciones apropiadas y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral.	Estos controles se encuentran en la Política de Seguridad de la Información. En el VAPS se hace referencia a la Política de Seguridad de la Información.	
	7.3. Controles de Personal - 7.3.4. Frecuencia y requisitos de las re-capacitaciones	Como mínimo las re-capacitaciones deben ser llevadas a cabo cuando existan cambios significativos en los elementos tratados en la capacitación inicial.	Estos controles se encuentran en la Política de Seguridad de la Información. En el VAPS se hace referencia a la Política de Seguridad de la Información.	
	7.3. Controles de Personal - 7.3.5. Frecuencia y secuencia de la rotación en el trabajo	El SVA debe establecer en su VAPS u otra documentación relevante si implementará políticas de rotación en el trabajo, en ese caso se debe establecer documentalmente los procedimientos necesarios, incluyendo los periodos mínimos para realizar la rotación.	No aplica	
	7.3. Controles de Personal - 7.3.6. Sanciones por acciones no autorizadas	Debe existir un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad. Como mínimo, en el caso de una acción real o potencial no autorizada, que haya sido realizada por una persona que desempeña un rol de confianza, dicha persona debe ser inmediatamente suspendida de todo rol de confianza que pudiera desempeñar.	Estos controles se encuentran en la Política de Seguridad de la Información. En el VAPS se hace referencia a la Política de Seguridad de la Información.	
	7.3. Controles de Personal - 7.3.7. Requerimientos de la contratación contratistas	Se debe establecer en la VAPS u otra documentación relevante, si es que se permite el empleo de contratistas.	Este tipo de controles se realiza en el documento que acredita la vinculación con un tercero, solicitado en la acreditación.	

	7.3. Controles de Personal - 7.3.8. Documentación suministrada al personal	Se debe entregar al personal la documentación necesaria para el desempeño de sus funciones.	Estos controles se encuentran en la Política de Seguridad de la Información. En el VAPS se hace referencia a la Política de Seguridad de la Información.	
	7.4. Procedimiento de registro de Auditorías - 7.4.1. Tipos de Eventos registrados	Se deben registrar todos los eventos significativos de seguridad y se deben detallar la fecha y hora exacta de su realización, la cual no debe estar posibilitada de ser eliminada ni modificada del registro.	Este procedimiento se encuentra en la Política de Seguridad de la Información. En el VAPS se hace referencia a la Política de Seguridad de la Información.	
	7.4. Procedimiento de registro de Auditorías - 7.4.2. Frecuencia del procesamiento del registro	Los registros de auditoría deben ser procesados y revisados una vez al mes como mínimo, con el fin de buscar actividades sospechosas o no habituales	Este procedimiento se encuentra en la Política de Seguridad de la Información. En el VAPS se hace referencia a la Política de Seguridad de la Información.	
	7.4. Procedimiento de registro de Auditorías - 7.4.3. Periodo de conservación del registro de auditorías	Los registros de auditorías deben conservarse por un periodo de siete años como mínimo.	Este procedimiento se encuentra en la Política de Seguridad de la Información. En el VAPS se hace referencia a la Política de Seguridad de la Información.	
	7.4. Procedimiento de registro de Auditorías - 7.4.4. Protección del registro de auditorías.	Los archivos donde se almacene la información relevante para las auditorías deben estar protegidos por listas de control de acceso que permitan solamente a los administradores del SVA tener acceso a esa información tanto para lectura como para escritura.	Este procedimiento se encuentra en la Política de Seguridad de la Información. En el VAPS se hace referencia a la Política de Seguridad de la Información.	
	7.4. Procedimiento de registro de Auditorías - 7.4.5. Procedimiento de copia de seguridad del registro de auditorías	Como mínimo debe realizarse de manera mensual una copia de seguridad del registro de auditorías, la cual debe archivarse fuera de las instalaciones.	Este procedimiento se encuentra en la Política de Seguridad de la Información. En el VAPS se hace referencia a la Política de Seguridad de la Información.	
	7.4. Procedimiento de registro de Auditorías - 7.4.6. Sistema de	Las auditorías internas deben llevarse a cabo, una vez cada 6 meses. Las auditorías externas deben llevarse a cabo una vez al año (auditoría periódica).	Este procedimiento se encuentra en la Política de Seguridad de la Información. En el VAPS se hace referencia a la Política de Seguridad	

	realización de auditoría (Interna vs Externa)		de la Información.	
	7.4. Procedimiento de registro de Auditorías - 7.4.7. Notificación al usuario que causa un evento	Se debe establecer en la RPS del SVA u otra documentación relevante si es que resulta factible realizar notificaciones a los usuarios que causan los eventos.	Este procedimiento se encuentra en la Política de Seguridad de la Información. En el VAPS se hace referencia a la Política de Seguridad de la Información.	
	7.4. Procedimiento de registro de Auditorías - 7.4.8. Valoración de vulnerabilidad	El SVA debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información en uso. Además, se debe evaluar el riesgo al que se expone la organización ante esas vulnerabilidades y se deben tomar medidas para reducir el impacto.	Este procedimiento se encuentra en la Política de Seguridad de la Información. En el VAPS se hace referencia a la Política de Seguridad de la Información.	
	7.5. Archivo de Registros - 7.5.1. Tipos de eventos registrados	Como mínimo debe mantenerse: la información del usuario, información firmada digitalmente y generada por los usuarios (en el caso del SIE) estado de inscripción ante INDECOPI, claves públicas del SVA y registro de auditorías.	Este procedimiento se encuentra en la Política de Seguridad de la Información. En el VAPS se hace referencia a la Política de Seguridad de la Información.	
	7.5. Archivo de Registros - 7.5.2. Periodo de conservación del archivo	Como mínimo, los archivos deben ser mantenidos por un periodo de diez (10) años. Las aplicaciones requeridas para tener acceso a un archivo deben también ser archivadas.	Este procedimiento se encuentra en la Política de Seguridad de la Información. En el VAPS se hace referencia a la Política de Seguridad de la Información.	
	7.5. Archivo de Registros - 7.5.3. Protección del archivo	Se debe establecer en la Política de Seguridad del SVA u otra documentación relevante las medidas de protección de la información archivada. Como mínimo las medidas deben prevenir cualquier modificación o eliminación de los datos contenidos en el archivo, e impedir el acceso a personas no autorizadas. Asimismo, debe garantizarse la confidencialidad de los datos proporcionados por los usuarios. Las medidas de seguridad que se adopten deben ser proporcionales a la sensibilidad e importancia de la información contenida en el archivo.	Este procedimiento se encuentra en la Política de Seguridad de la Información. En el VAPS se hace referencia a la Política de Seguridad de la Información.	
	7.5. Archivo de Registros -7.5.4.	Con el fin de mantener la integridad y disponibilidad de los servicios de procesamiento	Este procedimiento se encuentra en la Política de Seguridad de la	

	Procedimientos para copia de seguridad del archivo	de información y comunicaciones, se deben realizar copias de respaldo de la información y software esencial. Dichas copias deben ser probadas con regularidad. Los procedimientos deben ser compatibles con los estándares ISO mencionados en las referencias de esta sección o la generación de microformas de acuerdo al Decreto Legislativo 681.	Información. En el VAPS se hace referencia a la Política de Seguridad de la Información.	
	7.5. Archivo de Registros - 7.5.5. Requisitos para los archivos de sellado de tiempo	Los datos archivados deben consignar la fecha y hora, y la firma digital de la organización que genera dichos datos según la RFC 3161 (Time Stamping), o pueden ser protegidos de cualquier otra forma que pueda demostrar que los datos corresponden a la organización que los ha generado.	Este procedimiento se encuentra en la Política de Seguridad de la Información. En el VAPS se hace referencia a la Política de Seguridad de la Información.	
	7.5. Archivo de Registros - 7.5.6. Procedimiento para obtener y verificar la información del archivo	Los procedimientos para la obtención y verificación de la información del archivo deben encontrarse de conformidad con los requisitos de confidencialidad y privacidad de la Norma Marco de Privacidad, presentada en el anexo 5.	Este procedimiento se encuentra en la Política de Seguridad de la Información. En el VAPS se hace referencia a la Política de Seguridad de la Información.	
	7.6. Recuperación frente al compromiso y desastre - 7.6.1. Procedimiento de manejo de incidentes y compromisos	El plan de contingencias debe establecer de manera específica los procedimientos que deben seguirse en el caso de un evento o compromiso real o potencial de la integridad de las operaciones de los SVAs. Los eventos e incidentes que afecten la seguridad de la información deben reportarse al Responsable de Seguridad lo más rápidamente posible.	Este procedimiento se encuentra en la Política de Seguridad de la Información. En el VAPS se hace referencia a la Política de Seguridad de la Información.	
	7.6. Recuperación frente al compromiso y desastre - 7.6.2. Adulteración de los recursos computacionales, software y/o datos	El plan debe identificar fuentes alternativas de recursos computacionales, software y datos, las cuales deben ser empleadas en los casos de adulteraciones o fallas en los mismos.	Este procedimiento se encuentra en la Política de Seguridad de la Información. En el VAPS se hace referencia a la Política de Seguridad de la Información.	
	7.7. Finalización del	Se requiere información por parte de los PSCs	Esto se encuentra en el documento	

	SVA	respecto a operaciones de finalización (disolución) o transferencia de su titularidad. El SVA debe informar al INDECOPI, a los suscriptores, titulares y terceros que confían sobre el cese de sus operaciones con por lo menos treinta (30) días calendario de anticipación.	VAPS en el apartado “Finalización del SVA”	
CONTROLES DE SEGURIDAD TÉCNICA	8.1. Niveles de seguridad de los certificados y protección de la clave privada	Los certificados de autenticación emitidos por los SVAs deben cumplir como mínimo con los requerimientos del nivel de seguridad medio, establecidos en la Guía de Acreditación de SVA.	Este procedimiento se encuentra en la Política de Seguridad de la Información. En el VAPS se hace referencia a la Política de Seguridad de la Información.	
	8.2. Estándares y controles para el módulo criptográfico	Los módulos criptográficos usados por los SVAs deben cumplir los requerimientos de o ser equivalentes a FIPS 140-2 nivel de seguridad 2 o Common Criteria EAL 4+, como mínimo.	Este procedimiento se encuentra en la Política de Seguridad de la Información. En el VAPS se hace referencia a la Política de Seguridad de la Información.	
	8.3. Controles de Seguridad computacional - 8.3.1. Requisitos Técnicos específicos para seguridad computacional	El SVA debe establecer en su VAPS los controles de seguridad computacional y aquellos requeridos para los PSCs acreditados, incluyendo métodos necesarios para la evaluación de dichos controles.	Este procedimiento se encuentra en la Política de Seguridad de la Información. En el VAPS se hace referencia a la Política de Seguridad de la Información.	
	8.3. Controles de Seguridad computacional - 8.3.2. Evaluación de la seguridad computacional	Las evaluaciones deben ser realizadas de manera compatible con los siguientes estándares internacionales : a) La norma ISO/IEC 15408 “Information technology – Security techniques - Evaluation criteria for IT security”. b) La norma ISO/IEC 17799 “Information technology – Code of practice for information security management” y la norma ISO/IEC TR13335 “Information technology - Guidelines for the management of IT Security” c) La norma ISO/IEC 27001:2005 “Information technology - Security techniques - Information security management systems - Requirements”.	Este procedimiento se encuentra en la Política de Seguridad de la Información. En el VAPS se hace referencia a la Política de Seguridad de la Información.	

		d) FIPS PUB 140-2 – “Security Requirements for Cryptographic Modules” o Common Criteria EAL		
	8.4. Controles técnicos del ciclo de vida - 8.4.1. Controles de desarrollo del sistema	Se debe establecer en la VAPS u otra documentación relevante, los controles de desarrollo del sistema.	Este procedimiento se encuentra en la Política de Seguridad de la Información. En el VAPS se hace referencia a la Política de Seguridad de la Información.	
	8.4. Controles técnicos del ciclo de vida - 8.4.2. Controles de gestión de seguridad	Los controles para prevenir o detectar la modificación no autorizada del software o cambios en el sistema de configuración y la frecuencia de validación de la integridad del sistema deben ser establecidos conforme a la Guía de Acreditación de Software.	Este procedimiento se encuentra en la Política de Seguridad de la Información. En el VAPS se hace referencia a la Política de Seguridad de la Información.	
	8.4. Controles técnicos del ciclo de vida - 8.4.3. Evaluación de seguridad del ciclo de vida	Los controles de seguridad deben ser revisados como parte de la auditoría o evaluación de compatibilidad con la IOFE.	Este procedimiento se encuentra en la Política de Seguridad de la Información. En el VAPS se hace referencia a la Política de Seguridad de la Información.	
	8.5. Controles de seguridad de la red	La norma ISO/IEC 17799 “Information technology – Code of practice for information security management”, la norma ISO/IEC TR13335 “Information technology – Guidelines for the management of IT Security” y la norma ISO/IEC 27001:2005 “Information technology - Security techniques - Information security management systems - Requirements”, proveen directrices respecto a los tipos de controles que deben implementarse.	Este procedimiento se encuentra en la Política de Seguridad de la Información. En el VAPS se hace referencia a la Política de Seguridad de la Información.	
	8.6. Sello de tiempo	Se admiten servicios de sellado de hora y tiempo según la norma ISO/IEC 18014-1:2000 “Information technology -- Security techniques – Timestamping Services -- Part 1: Framework”. Para tales efectos debe emplearse una fuente confiable de tiempo.	Se especifica en el VAPS que efectivamente se puede aplicar este tipo de servicio dentro de la intermediación electrónica.	
AUDITORÍAS DE COMPATIBILIDAD Y OTRAS	9.1. Frecuencia y circunstancias de la evaluación.	Los SVAs deben someterse una vez al año a auditorías o evaluaciones de conformidad respecto del marco de la IOFE.	Este procedimiento se encuentra en la Política de Seguridad de la Información. En el VAPS se hace	

EVALUACIONES			referencia a la Política de Seguridad de la Información.	
	9.2. Identidad/ Calificaciones de asesores	Un equipo de auditoría o evaluación de compatibilidad debe incluir a personas con experiencia significativa en tecnologías de la información, seguridad y tecnologías de PKI y criptográficas.	Este procedimiento se encuentra en la Política de Seguridad de la Información. En el VAPS se hace referencia a la Política de Seguridad de la Información.	
	9.3. Relación del auditor con la entidad auditada	Los auditores o asesores deben ser independientes de la organización que auditan o evalúan.	Este procedimiento se encuentra en la Política de Seguridad de la Información. En el VAPS se hace referencia a la Política de Seguridad de la Información.	
	9.4. Elementos cubiertos por la evaluación	Los elementos cubiertos por la auditoría son la implementación de las prácticas de personal, procedimientos y técnicas descritas en este documento.	Este procedimiento se encuentra en la Política de Seguridad de la Información. En el VAPS se hace referencia a la Política de Seguridad de la Información.	
	9.5. Acciones a ser tomadas frente a resultados deficientes	Al detectarse una irregularidad, y dependiendo de la gravedad de la misma, podrán tomarse entre otras las siguientes acciones: a) Indicar las irregularidades, pero permitir al SVA que continúe sus operaciones hasta la próxima auditoría programada. b) Permitir al SVA que continúe sus operaciones por un máximo de treinta (30) días útiles pendientes a la corrección de los problemas antes de suspenderlo. c) Suspender las operaciones del SVA.	Este procedimiento se encuentra en la Política de Seguridad de la Información. En el VAPS se hace referencia a la Política de Seguridad de la Información.	
	9.6. Publicación de Resultados	Los resultados de las auditorías o evaluaciones de compatibilidad bajo el marco de la IOFE de los SVAs deben ser publicados como parte de la información de estado de aquellas entidades, la cual es publicada por INDECOPI.	Se especifica en el VAPS que se entregara dicha información a la IOFE.	
OTRAS MATERIAS DE NEGOCIO Y LEGALES	10.1. Política de reembolso	El SVA debe establecer en su VAPS, sus olíticas de reembolso. En particular, las políticas deben estar establecidas o referenciadas en los contratos de sus usuarios y terceros que confían	Esto se encuentra en el documento VAPS en el apartado “13. POLÍTICA DE REEMBOLSO”	
	10.2.Confidencialidad	Las categorías de información que deben de ser	Esto se maneja en los documentos de	

	de la información del negocio	mantenidas de manera confidencial se encuentran especificadas en la Norma Marco sobre Privacidad, el cual se encuentra en el anexo 5.	Política y Plan de Privacidad de Datos Personales.	
	10.3. Alcances de la información confidencial	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	Esto se maneja en los documentos de Política y Plan de Privacidad de Datos Personales.	
	10.4. Responsabilidad de protección de la Información confidencial - 10.4.1. Privacidad de la información personal	Los SVAs deben cumplir tanto sus requisitos de confidencialidad como las leyes sobre protección de datos, confidencialidad de la información y propiedad intelectual que les fueran aplicables.	Esto se maneja en los documentos de Política y Plan de Privacidad de Datos Personales.	
	10.4. Responsabilidad de protección de la Información confidencial - 10.4.2. Política y Plan de privacidad	Se requiere de los SVAs la preparación de una Política de Privacidad y un Plan de Privacidad de conformidad con la Norma Marco sobre Privacidad presentada en el anexo 5, sujetos a las existentes obligaciones contractuales, licencias u otros arreglos de outsourcing.	Esto se maneja en los documentos de Política y Plan de Privacidad de Datos Personales.	
	10.4. Responsabilidad de protección de la Información confidencial - 10.4.3. Información tratada como privada	Los SVAs deben cumplir tanto sus requisitos de confidencialidad como las leyes sobre protección de datos, confidencialidad de la información y propiedad intelectual que les fueran aplicables.	Esto se maneja en los documentos de Política y Plan de Privacidad de Datos Personales.	
	10.4. Responsabilidad de protección de la Información confidencial - 10.4.4.	Los SVAs deben cumplir con la legislación sobre protección de datos de conformidad con la Norma Marco sobre Privacidad que se encuentra en el anexo 5. También debe tomarse en consideración la	Esto se maneja en los documentos de Política y Plan de Privacidad de Datos Personales.	

	Información no considerada privada	legislación sobre protección de datos de las jurisdicciones con las que mantengan acuerdos de reconocimiento cruzado y las políticas de protección de datos personales existentes en dichas infraestructuras.		
	10.4. Responsabilidad de protección de la Información confidencial - 10.4.5. Responsabilidad de protección de la información privada	Se requiere de los SVAs la preparación de una Política de Privacidad y un Plan de Privacidad de conformidad con la Norma Marco sobre Privacidad presentada en el anexo 5, sujetos a las existentes obligaciones contractuales, licencias u otros arreglos de outsourcing.	Esto se maneja en los documentos de Política y Plan de Privacidad de Datos Personales.	
	10.4. Responsabilidad de protección de la Información confidencial - 10.4.6. Notificación y consentimiento para el uso de información	En los acuerdos que serán firmados por los usuarios se debe establecer el tipo de datos personales que pueden ser recolectados, cómo serán utilizados, protegidos y cómo estos pueden ser revisados/corregidos, las circunstancias bajo las cuales serán divulgados, la manera de desagravios y sanciones para las fallas en el cumplimiento del acuerdo con la parte o partes que utilizan o recolectan dichos datos. Asimismo debe incorporarse en el acuerdo, el necesario consentimiento para la divulgación de datos específicos.	Esto se maneja en los documentos de Política y Plan de Privacidad de Datos Personales.	
	10.4. Responsabilidad de protección de la Información confidencial - 10.4.7. Divulgación realizada con motivo de un proceso judicial o administrativo	Se permite la divulgación de información personal sólo en los casos en que exista consentimiento expreso del individuo cuya información corresponde.	Esto se maneja en los documentos de Política y Plan de Privacidad de Datos Personales.	
	10.4. Responsabilidad de protección de la	Las categorías de información personal que deben ser mantenidas de manera confidencial y las circunstancias bajo las cuales dicha	Esto se maneja en los documentos de Política y Plan de Privacidad de Datos Personales.	

	Información confidencial - 10.4.8. Otras circunstancias para divulgación de información	información puede ser revelada deben estar de conformidad con la Norma Marco sobre Privacidad presentada en el anexo 5 de la Guía de Acreditación de EC.		
	10.5. Derechos de propiedad intelectual	En los acuerdos que serán firmados por los usuarios se debe establecer el tipo de datos personales que pueden ser recolectados, cómo serán utilizados, protegidos y cómo estos pueden ser revisados/corregidos, las circunstancias bajo las cuales serán divulgados, la manera de desagravios y sanciones para las fallas en el cumplimiento del acuerdo con la parte o partes que utilizan o recolectan dichos datos. Asimismo debe incorporarse en el acuerdo, el necesario consentimiento para la divulgación de datos específicos.	Esto se maneja en los documentos de Política y Plan de Privacidad de Datos Personales.	
	10.6. Responsabilidad Financiera - 10.6.1. Cobertura de seguro	Los SVAs deberán presentar para su acreditación, documentación que respalde la contratación de seguros o garantías bancarias para salvaguardar sus actividades. El monto mínimo de la póliza es de $ 35 000.00 dólares americanos.	Este apartado se especifica en detalle en la consulta realizada a INDECOPI el día 03/04/2017 con referencia a la Formulación de Consulta en relación a la obligación de los Prestadores de Servicios de Valor Añadido (SVA) de contratar seguros o garantías bancarias.	
	10.7. Representaciones y garantías - 10.7.1. Representaciones y garantías del SVA	El SVA debe establecer en su VAPS, provisiones de garantía y responsabilidad, incluyendo limitaciones y exclusiones. Debe asimismo asegurar que dichas provisiones se encuentren establecidas en los contratos de usuario y tercero que confía (según sea el caso).	Esto se especifica en el VAPS en el apartado ”Responsabilidad Financiera, Representaciones Y Garantías”	
	10.7. Representaciones y garantías - 10.7.2. Representaciones y garantías de los usuarios	Un usuario o titular está obligado a cumplir las obligaciones de usuario establecidas en el SVA. Se debe requerir al usuario la firma de un acuerdo de cumplimiento de sus obligaciones, incluyendo las concernientes a los titulares inscritos por él. El acuerdo debe incluir las consecuencias de eventuales incumplimientos.	Esto se especifica en el VAPS en el apartado ”Responsabilidad Financiera, Representaciones Y Garantías”	
	10.7.	Una tercero que confía es compelida a cumplir	Esto se especifica en el VAPS en el	

	Representaciones y garantías - 10.7.3. Representaciones y garantías de los terceros que confían (terceros usuarios)	con sus obligaciones establecidas en la VAPS. Se le debe notificar al tercero que confía dichas obligaciones por intermedio de la publicación de un documento accesible al él. El documento debe incluir las consecuencias derivadas del incumplimiento del acuerdo.	apartado ”Responsabilidad Financiera, Representaciones Y Garantías”	
	10.7. Representaciones y garantías - 10.7.4. Representaciones y garantías de otros participantes	El repositorio y otros participantes no específicamente mencionados anteriormente, deben establecer en su Declaración de Prácticas de Prestación de Servicios de Valor Añadido u otra documentación provisiones sobre garantías y responsabilidades, incluyendo limitaciones y exclusiones de las mismas. Asimismo deben asegurar que dichas provisiones se incluyan en todo contrato de usuario o tercero que confía.	Esto se especifica en el VAPS en el apartado ”Responsabilidad Financiera, Representaciones Y Garantías”	
	10.7. Representaciones y garantías - 10.7.5. Exención de garantías	Los SVAs deben establecer en sus VAPS, cualquier exención de responsabilidad que pudiera aplicárseles. Asimismo deben asegurar que estas provisiones sean incluidas en cualquier contrato de usuario y tercero que confía.	Esto se especifica en el VAPS	
	10.7. Representaciones y garantías - 10.7.6. Limitaciones a la responsabilidad	Los SVAs deben establecer en su VAPS u otra documentación relevante, cualquier limitación de responsabilidad que pudiera aplicárseles, considerando las responsabilidades de privacidad, seguridad y diligencia en los procesos de certificación que INDECOPI establece en este documento. Asimismo deben asegurar que estas provisiones sean incluidas en cualquier contrato de usuario o tercero que confía.	Esto se especifica en el VAPS	
	10.8. Indemnizaciones	Los SVAs deben establecer en sus VAPS, lo relativo a las indemnizaciones a las que pudieran estar sujetos. Asimismo debe asegurar que estas provisiones sean incluidas en cualquier contrato de suscriptor o tercero que confía.	Esto se especifica en el VAPS en el apartado ”Indemnizaciones”	
	10.9. Término y terminación - 10.9.1. Término	El periodo máximo de habilitación de las funciones relativas a los SVAs acreditados es de tres (3) años, de acuerdo a la legislación vigente.	Esto se encuentra en el documento VAPS en el apartado “Finalización del SVA”	
	10.9. Término y	Los procedimientos necesarios para el cese de	Esto se encuentra en el documento	

	terminación - 10.9.2. Terminación	las operaciones de un SVA y el plazo en el cual dicha entidad deberá notificar sus intenciones de terminación tanto a INDECOPI, suscriptores y terceros que confían; serán establecidos por la Comisión de Reglamentos Técnicos y Comerciales de INDECOPI, en conformidad a la legislación vigente.	VAPS en el apartado “Finalización del SVA”	
	10.9. Término y terminación - 10.9.3. Efecto de terminación y supervivencia	Los SVAs deberán establecer, en sus modelos de contratos de usuarios y terceros que confían (según sea el caso), cláusulas de supervivencia, de modo que ciertas reglas continúen vigentes después de la finalización de la VAPS y de los contratos de los suscriptores y terceros que confían. En particular, deben continuar operativas las reglas relativas a la privacidad y propiedad intelectual.	Esto se encuentra en el documento VAPS en el apartado “Finalización del SVA”	
	10.10. Notificaciones y Comunicaciones individuales con los participantes - 10.10.1. Enmendaduras	Los SVAs deben establecer, en sus contratos de suscriptor y terceros que confían, cláusulas de notificación que regulen los procedimientos por los que las partes se notifiquen hechos mutuamente.	Esto se encuentra en el documento VAPS en el apartado “Enmendaduras”	
	10.10. Notificaciones y Comunicaciones individuales con los participantes - 10.10.2. Procedimiento para enmendaduras	Los participantes de la IOFE, incluyendo las otras infraestructuras que lo reconocen, serán consultados antes de efectuar cualquier tipo de cambio en los documentos de la infraestructura. Esta provisión no se aplica a cambios de las políticas y prácticas de los PSCs acreditados, cuando dichos cambios son consistentes con las operaciones documentadas de la propia IOFE.	Esto se encuentra en el documento VAPS en el apartado “Enmendaduras”	
	10.10. Notificaciones y Comunicaciones individuales con los participantes - 10.10.3. Mecanismos y periodo de	Los cambios en las políticas y prácticas de los PSCs acreditados deben ser notificados a los usuarios y terceros que confían, cuando dichos cambios puedan afectarles.	Este procedimiento se encuentra en la Política de Seguridad de la Información. En el VAPS se hace referencia a la Política de Seguridad de la Información.	

	notificación			
	10.11. Provisiones sobre resolución de disputas	Los SVAs deben establecer procedimientos de resolución de disputas en su VAPS otra documentación relevante. De ser posible y permitido por las leyes correspondientes, debe considerarse el empleo de resolución de disputas en línea.	Esto se encuentra en el documento VAPS en el apartado “Resolución de Disputas”	
	10.12. Ley aplicable	El SVA debe identificar en su VAPS y otra documentación relevante las leyes y normas aplicables a sus operaciones de acuerdo a la Ley 27269 y el Reglamento de Ley de Firmas y Certificados Digitales 004-2007 PCM.	Esto se encuentra en el documento VAPS en el apartado “Resolución de Disputas”	
	10.13. Conformidad con la ley aplicable	El SVA debe identificar en su VAPS y otra documentación relevante la ley aplicable a sus operaciones de acuerdo a la Ley 27269 y el Reglamento de Ley de Firmas y Certificados Digitales 004-2007 PCM y otros.	Esto se encuentra en el documento VAPS en el apartado “Resolución de Disputas”	
	10.14. Provisiones Misceláneas - 10.14.1. Acuerdo completo	El SVA debe incluir en su VAPS toda provisión miscelánea que se aplique a las operaciones que realiza bajo la IOFE. De ser apropiado, estas provisiones deben ser establecidas o referenciadas en los contratos de usuarios o terceros que confían.	Esto se encuentra en el documento VAPS	
	10.14. Provisiones Misceláneas - 10.14.2. Subrogación	Se debe hacer referencia en cada acuerdo de acreditación para los PSCs acreditados de cualquier otra documentación que pueda ser incorporada en el acuerdo.	Esto se encuentra en el documento VAPS	
	10.14. Provisiones Misceláneas - 10.14.3. Divisibilidad	Los derechos y los deberes asociados a la condición de EC, ER o SVA no podrán ser objeto de cesión a terceros de ningún tipo, ni ninguna tercera entidad podrá subrogarse en la posición jurídica de dichas entidades.	Esto se encuentra en el documento VAPS	
	10.14. Provisiones Misceláneas - 10.14.4. Ejecución (tarifas de abogados y cláusulas de derechos)	El SVA debe establecer en su VAPS y otra documentación relevante toda provisión de ejecución que se aplique a las operaciones que realiza. Estas provisiones deben estar establecidas o referenciadas en los contratos de usuario y tercero que confía.	Esto se encuentra en el documento VAPS en la sección “Tarifas”	
	10.14. Provisiones	Las provisiones de “fuerza mayor” están limitadas	Esto se encuentra en el documento	

	Misceláneas - 10.14.5. Fuerza mayor	por los requisitos necesarios para la acreditación de un SVA bajo la IOFE para los planes de continuidad de negocio que establezcan eventos que puedan ser considerados como de “fuerza mayor”.	VAPS en la sección “Fuerza Mayor y Otras Provisiones”	
	10.15. Otras provisiones	El SVA debe incluir en su VAPS cualquier otra provisión que se aplique a las operaciones que realiza bajo la IOFE. Cuando fuere apropiado, estas provisiones deben estar establecidas o referenciadas en el acuerdo de los usuarios o terceros que confían.	Esto se encuentra en el documento VAPS en la sección “Fuerza Mayor y Otras Provisiones”	
	11. BIBLIOGRAFÍA	La VAPS debe establecer las referencias a los documentos utilizados en el desarrollo de dicha documentación. Particularmente, aquellos documentos referenciados en la documentación o que hacen mención a algún tipo de norma o regulación en particular.	Esto se encuentra en el documento VAPS.	
	12. ACRÓNIMOS & ABREVIATURAS	La VAPS debe proveer una lista de acrónimos y abreviaturas utilizadas dentro del texto de dicha documentación.	Esto se encuentra en el documento VAPS.	
	13. GLOSARIO	La VAPS debe proveer una lista de términos para los cuales pueda ser requerida una definición.	Esto se encuentra en el documento VAPS.	