AUTORIDAD DE INTERMEDIACIÓN ELECTRÓNICA	Fecha: 12/06/2020
	Versión: 2

DECLARACIÓN DE PRÁCTICAS DE VALOR AÑADIDO

SISTEMA DE INTERMEDIACIÓN ELECTRONICA - PLUSSIGNER

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
Angela Donayre (Jefe de Infraestructura)	24/04/2018	2
José Junior Damian Tirado (Jefe de Aplicaciones y Desarrollo)	10/05/2019	2
José Junior Damian Tirado (Gerente General / Arquitecto de Soluciones)	08/06/2020	2

Cambios	Fecha de Revisión	Versión	Cambios Realizados
Jesús Ojeda (Oficial de Seguridad)	02/03/2017	2	Realización del Documento
José Damian Tirado.	18/04/2018	2	Cambios en la especificación de las responsabilidades de reembolso, así como financieras y de garantía. Cambios en agregar funcionalidades de la plataforma.
José Junior Damian Tirado	07/05/2019	2	Cambios en la Responsabilidad del Suscriptor. Cambios en la especificación de las responsabilidades de reembolso, así como financieras y de garantía. Cambios en agregar funcionalidades de la plataforma.
José Junior Damian Tirado	01/06/2020	2	Cambios en la especificación de las responsabilidades de reembolso, así como financieras y de garantía. Cambios en agregar funcionalidades de la plataforma. Cambios en la parte de terceros que confían. Se agrego el apartado de Notificaciones y Comunicaciones entre participantes.

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 Plan de contingencia de TI 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 la descripción de las operaciones y prácticas que utiliza PLUSSIGNER para la administración de sus servicios como Prestador de Servicios de Valor Añadido tipo Sistema de Intermediación Digital, 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.

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. DEFINICIONES Y ABREVIACIONES

- **Acceso:** Es la lectura o grabación de datos que han sido almacenados en un sistema de computación. Cuando se consulta una Base de Datos, los datos son primero accedidos y suministrados a la computadora y luego transmitidos a la pantalla del equipo.
- **Amenaza:** Cualquier evento que pueda interferir con el funcionamiento de un computador o causar la difusión no autorizada de información confiada a un computador. Ejemplo: Fallas del suministro eléctrico, virus, saboteos o descuido del usuario.
- **Ataque:** Término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático o el intento de obtener de modo no autorizado la información confiada a un computador.
- **Base de Datos:** Es un conjunto de datos organizados, entre los cuales existe una correlación y que además están almacenados con criterios independientes de los programas que los utilizan. Entre sus principales características se encuentran brindar seguridad e integridad a los datos, proveer lenguajes de consulta, de captura y edición de los datos en forma interactiva, proveer independencia de los datos.
- **Datos:** Los datos son hechos y/o valores que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos en el presente documento. En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y Bases de Datos, textos (colección de palabras), hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), videos (secuencia de tramas), etc.
- **Golpe (Breach):** Es la violación exitosa de las medidas de seguridad, como el robo de información, la eliminación de archivos de datos valiosos, el robo de equipos, PC, etc.
- **Incidente:** Cuando se produce un ataque o se materializa una amenaza se tiene un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de eliminación de un archivo protegido.
- **Integridad:** Los valores consignados en los datos se han de mantener de tal manera que representen la realidad y su modificación debe ser registrada en bitácoras del sistema que permitan la auditoría de los acontecimientos. Las técnicas de integridad sirven para prevenir el ingreso de valores errados en los datos sea esta situación provocada por el software de la Base de Datos, por fallas de los programas, del sistema, el hardware o, simplemente, por errores humanos.
- **Privacidad:** Se define como el derecho que tiene el COPNIA para determinar, a quién, cuándo y qué información de su propiedad podrá ser difundida o transmitida a terceros.
- **Seguridad:** Se refiere a las medidas que toma el COPNIA con el objeto de preservar la integridad de sus datos o información procurando que no sean modificados, destruidos o divulgados ya sea en forma accidental, no autorizada o intencional. En el caso de los datos e información contenidos en los sistemas de información del COPNIA, la privacidad y seguridad guardan estrecha relación entre sí, aunque la diferencia entre ellas radica en que la primera se refiere a la distribución autorizada de información y la segunda al acceso no autorizado.

- **Sistemas de Información:** Es el término empleado en el ambiente del procesamiento de datos para referirse al almacenamiento de los datos de una organización y ponerlos a disposición de su personal. Pueden ser registros simples como archivos de Word y Excel, o pueden ser complejos como una aplicación de software con base de datos.
- **Cortafuegos (Firewall):** Es un sistema diseñado para bloquear el acceso no autorizado de comunicaciones. Se trata de un dispositivo configurado para permitir, limitar, cifrar y descifrar el tráfico de mensajes entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios. Los cortafuegos se utilizan para evitar que los usuarios.
- **Plan de Contingencia:** Son procedimientos que definen cómo una entidad continuará o recuperará sus funciones críticas en caso de una interrupción no planeada.
- **Riesgo:** Es la vulnerabilidad de un Activo o bien, ante un posible o potencial perjuicio o daño.

- **Infraestructura Oficial de Firma Electrónica (IOFE):** sistema confiable, acreditado, regulado y supervisado por la Autoridad Administrativa Competente, provisto de instrumentos legales y técnicos que permiten generar firmas electrónicas y proporcionar diversos niveles de seguridad respecto a: 1) la integridad de los mensajes de datos y documentos electrónicos; 2) la identidad de su autor, lo que es regulado conforme a la Ley. El sistema incluye la generación de firmas electrónicas, en la que participan entidades de certificación y entidades de registro o verificación acreditadas ante la Autoridad Administrativa Competente incluyendo a la Entidad de Certificación Nacional para el Estado Peruano (ECERNEP), las Entidades de Certificación para el Estado Peruano (ECEP) y las Entidades de Registro o Verificación para el Estado Peruano (EREP).
- **Autenticación**: proceso técnico que permite determinar la identidad de la persona que firma electrónicamente, en función del mensaje firmado por éste y al cual se le vincula, este proceso no otorga certificación notarial ni fe pública.
- **Autoridad Administrativa Competente (AAC):** organismo público responsable de acreditar a las entidades de certificación y a las entidades de registro o verificación, de reconocer los estándares tecnológicos aplicables en la Infraestructura Oficial de Firma Electrónica, de supervisar dicha Infraestructura y las otras funciones señaladas en el Reglamento o aquellas que requiera en el transcurso de sus operaciones. Dicha responsabilidad recae en el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual – INDECOPI.
- **Certificado digital:** documento electrónico generado y firmado digitalmente por una entidad de certificación el cual vincula un par de claves con una persona natural o jurídica confirmando su identidad.
- **Clave privada:** es una de las claves de un sistema de criptografía asimétrica que se emplea para generar una firma digital sobre un mensaje de datos y es mantenida en reserva por el titular de la firma digital.
- **Clave pública:** es la otra clave en un sistema de criptografía asimétrica que es usada por el destinatario de un mensaje de datos para verificar la firma digital puesta en dicho mensaje. La clave pública puede ser conocida por cualquier persona.
- **Código de verificación (hash o resumen):** secuencia de bits de longitud fija obtenida como resultado de procesar un mensaje de datos con un algoritmo, de tal manera que: (1) El mensaje de datos produzca siempre el mismo código de verificación cada vez que se le aplique dicho algoritmo. (2) Sea improbable, a través de medios técnicos, que el mensaje de datos pueda ser derivado o reconstruido a partir del código de verificación producido por el algoritmo. (3)

Sea improbable que, por medios técnicos, se pueda encontrar dos mensajes de datos que produzcan el mismo código de verificación al usar el mismo algoritmo.

- **Criptografía asimétrica:** rama de las matemáticas aplicadas que se ocupa de transformar mensajes en formas aparentemente ininteligibles y devolverlas a su forma original, las cuales se basan en el empleo de funciones algorítmicas para generar dos “claves” diferentes pero matemáticamente relacionadas entre sí. Una de esas claves se utiliza para crear una firma numérica o transformar datos en una forma aparentemente ininteligible (clave privada) y la otra para verificar una firma numérica o devolver el mensaje a su forma original (clave pública). Las claves están matemáticamente relacionadas de tal modo que cualquier de ellas implica la existencia de la otra, pero la posibilidad de acceder a la clave privada a partir de la pública es técnicamente ínfima.
- **Depósito de certificados:** sistema de almacenamiento y recuperación de certificados, así como de la información relativa a éstos, disponible por medios telemáticos.
- **Destinatario:** persona designada por el iniciador para recibir un mensaje de datos o un documento electrónico siempre y cuando no actúe a título de intermediario.
- **Documento:** cualquier escrito público o privado, los impresos, fotocopias, facsímil o fax, planos, cuadros, dibujos, fotografías, radiografías, cintas cinematográficas, microformas tanto en la modalidad de microfilm como en la modalidad de soportes informáticos y otras reproducciones de audio o video, la telemática en general y demás objetos que recojan, contengan o representen algún hecho o una actividad humana o su resultado. Los documentos pueden ser archivados a través de medios electrónicos, ópticos o cualquier otro similar.
- **Tercero que confía o tercer usuario:** se refiere a las personas físicas, equipos, servicios o cualquier otro ente que actúa basado en la confianza sobre la validez de un certificado emitido por un certificado específico y/o verifica alguna firma digital en la que se utilizó dicho certificado.
- **Titular de certificado digital:** persona natural o jurídica a quien se le atribuye de manera exclusiva un certificado digital.

5. RESPONSABILIDADES Y OBLIGACIONES SUBSCRIPTOR

El suscriptor es la entidad o persona que adquiere el sistema de intermediación electrónica, hace uso de la plataforma y tiene ciertas responsabilidades y derechos en ella, los cuales se mencionarán a continuación, estas se dividen en dos partes (como producto y como servicio):

Como Producto:

Las responsabilidades y/o obligaciones son las siguientes:

- El suscriptor es dueño del componente, dependiendo la licencia que se está activando, el tipo puede variar.
- El suscriptor pueden hacer uso de la herramienta en base a las necesidades plasmadas brindadas en el contrato realizado con la organización.
- El suscriptor no puede modificar ningún archivo ni contenido de la herramienta, por lo que la empresa no se hace responsable de algún problema sobre error u omisión del usuario.
- El suscriptor no puede copiar el contenido de la herramienta, sin previa autorización de la empresa contratada, ante cualquier manipulación y copiado no autorizado, se manejarán procedimientos legales que garanticen el producto brindado al cliente.
- El suscriptor debe entregar cierta información solicitada por la empresa para hacer uso del producto, bajo un acuerdo de confidencialidad (NDA).
- El suscriptor no debe compartir las credenciales del producto, cualquier acción mal intencionada deberá ser sancionada y penalizada.
- Dependiendo el tipo de licencia el suscriptor tendrá acceso a actualizaciones, parches, mejoras, nuevas funciones y/o incorporaciones de nuevos servicios, según sea el caso.
- El suscriptor debe regirse a la política de seguridad, a la privacidad y protección de la información personal. Cualquier divulgación de la información fuera de la plataforma será sancionada y se penalizará por atentar contra el prejuicio de la entidad.
- Limitación de responsabilidad: SAETA no se hará responsable de los daños sufridos como resultado del uso, modificación, contribución, copia, distribución o descarga de los materiales en el producto. SAETA no se hará responsable de ningún daño indirecto, accidental, punitivo, especial o consecuente (incluida la pérdida de negocio, ingresos, beneficios, uso, datos u otras ventajas económicas) cualquiera que sea su causa, ya sea por incumplimiento o por acto ilícito, aunque SAETA haya sido advertido previamente de la posibilidad de este daño.

Como Servicio:

Las responsabilidades y/o obligaciones del suscriptor son las siguientes:

- El suscriptor no debe compartir sus credenciales y accesos a la plataforma como servicio, cualquier manipulación o uso indebido, será responsabilidad del mismo.
- El suscriptor debe acatar las responsabilidades del uso de la plataforma, así como respetar las licencias pactadas con el contratante previamente a la firma del contrato.
- Cualquier parte del servicio que no haya sido divulgada públicamente no se podrá divulgar ni comentar, excepto dentro del servicio otorgado, hasta que sea anunciada por la organización.
- El suscriptor tiene derecho a actualizaciones, parches, mejoras, nuevas funciones y/o incorporaciones de nuevos servicios, según sea el caso y la variante de la licencia.
- El suscriptor debe regirse a la política de seguridad, a la privacidad y protección de la información personal. Cualquier divulgación de la información fuera de la plataforma será sancionada y se penalizará por atentar contra el prejuicio de la entidad.
- El suscriptor firma un acuerdo de confidencialidad con SAETA donde se estipulan la protección de datos personales, los cuales deben estar constatados en dicho acuerdo.
- Limitación de responsabilidad: SAETA no se hará responsable de los daños sufridos como resultado del uso, modificación, contribución, copia, distribución o descarga de los materiales en el servicio. SAETA no se hará responsable de ningún daño indirecto, accidental, punitivo, especial o consecuente (incluida la pérdida de negocio, ingresos, beneficios, uso, datos u otras ventajas económicas) cualquiera que sea su causa, ya sea por incumplimiento o por acto ilícito, aunque SAETA haya sido advertido previamente de la posibilidad de este daño. acepta usted eximir a SAETA de cualquier responsabilidad y no demandar a SAETA por ninguna reclamación derivada de su uso del servicio o los materiales o servicios suministrados a través del servicio.

6. RESPONSABILIDADES Y OBLIGACIONES DE LA PSVA

La entidad PSVA debe velar por el buen funcionamiento de la plataforma de Intermediación electrónica y debe garantizar ciertas cualidades dentro de la adquisición tanto como producto y como servicio, a continuación se muestra los siguientes ítems:

- El suministro del producto y/o servicio está sujeto a las siguientes Condiciones de Uso. SAETA se reserva el derecho de actualizar las CDU en cualquier momento y sin previo aviso.
- Los servicios y/o productos le proporciona acceso a una variedad de recursos, incluidas herramientas de desarrollador, áreas de descarga, foros de comunicación e información de productos (colectivamente, los "Servicios"). Los Servicios, incluidas las actualizaciones, mejoras, nuevas funciones y/o la incorporación de nuevos servicios, están sujetos a las condiciones de Uso.

- La Entidad PSVA vela por la privacidad y protección de la información personal en relación del documento de privacidad y plan de seguridad de la información.
- RESTRICCIÓN DE USO PERSONAL Y NO COMERCIAL: A menos que se especifique lo contrario, los Servicios son para su uso personal y no comercial. No podrá modificar, copiar, distribuir, transmitir, mostrar, realizar, reproducir, publicar, autorizar, crear trabajos derivados, transferir ni vender información, software y/o productos o servicios obtenidos de los Servicios.
- MEDIDAS CAUTELARES: Usted reconoce que cualquier uso de los Servicios suministrados el servicio y/o producto contrario la presente Contrato, o cualquier transferencia, sub licencia, copia o divulgación de información técnica o Materiales relacionados con los servicios ofrecidos, pueden causar daños irreparables a SAETA, sus filiales, proveedores y otros terceros autorizados por SAETA para revender, distribuir o promocionar los servicios suministrados en esta página web ("Revendedores"), y en estas circunstancias, SAETA, sus filiales, proveedores y Revendedores tendrán derecho a una compensación equitativa, sin depositar ninguna fianza ni otra garantía, incluidas, entre otras, las medidas cautelares preliminares y permanentes.
- La PSVA debe brindar las credenciales para el acceso a la plataforma ya sea como producto o servicio, de manera segura, basándose en links de acceso.
- La PSVA debe brindar acceso y disponibilidad de la plataforma, basándose en las cláusulas del contrato a firmar con el suscriptor.
- La PSVA debe brindar la documentación necesaria para el correcto funcionamiento de la plataforma, los cuales mínimamente son los siguientes:
    - Manual de Usuario.
    - Manual de Operación.
    - Manual de Arquitectura.
- La PSVA debe brindar un canal de soporte ya sea por teléfono, correo electrónico y/o mesa de ayuda, que permita al usuario solicitar atención en caso de algún problema o mejora.
- La PSVA debe garantizar dentro de la plataforma los datos guardados así como garantizar la confidencialidad de la información.
- La PSVA debe garantizar el uso de canales SSL, así como la protección de los datos a través de la plataforma.
- La PSVA debe entregar reportes de trazabilidad y de auditoría en caso algún ente regulador realice alguna función fiscalizadora.

7. COMUNIDAD DE USUARIOS

Soluciones Aplicadas en Tecnología Avanzada S.A.C. brinda sus servicios de valor añadido a personas jurídicas y naturales del sector privado y gubernamental. Los cuales deben contar con lo siguiente:

- Personas naturales deben poseer un certificado digital vigente y emitido por una EC acreditada, reconocida por la IOFE o en el caso de certificados de autenticación, emitido por el SVA.

- Personas jurídicas cuyo suscriptor (aspirante a ser usuario del servicio) posea un certificado digital vigente emitido por una EC acreditada, reconocida por la IOFE o en el caso de certificados de autenticación, emitido por el SVA.

8. TERCEROS QUE CONFÍAN

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.

8.1. RESPONSABILIDADES Y OBLIGACIONES DE LOS TERCEROS QUE CONFIAN

El tercero que confía tiene las siguientes responsabilidades respecto al servicio o producto que brindamos:

- Deben verificar la validez de los certificados digitales de los documentos o información procesada por los sistemas de intermediación electrónica, para eso PSVA brinda mecanismos de verificación de la plataforma.
- Deben validar y tomar en cuenta cualquier limitación en el uso de los sistemas consideras en la DPSVA, por lo cual la PSVA no se hace responsable por cualquier proceso como tal.
- Debe respetar los acuerdos u obligaciones que se tengan en la plataforma así como realizar las actividades también estipuladas en la misma.

9. PLATAFORMA

Plussigner es una plataforma de intermediación electrónica creado con la finalidad de ofrecer una herramienta de creación y administración de documentos o archivos electrónicos de fácil operación siendo una solución que incluye firma electrónica con un certificado dependiendo el tipo de firma y su posterior publicación en la plataforma de custodia y verificación.

La plataforma de custodia permite archivar los documentos electrónicos generados:

- Posibilita el archivo electrónico de los documentos en una plataforma web

- Los usuarios tendrán una zona web de la que podrán descargarse copias auténticas de sus documentos o archivos, tanto en formato original como en formato imprimible.
- Terceros interesados podrán verificar los documentos en papel presentados por los usuarios, introduciendo el código de verificación impreso en el título.

Permite la firma y sellado de larga duración, mediante certificado reconocido, se almacenan las evidencias necesarias para la verificación de la firma electrónica a lo largo del tiempo.

La petición de sello de tiempo está conforme a la RFC 3161 y brinda los estándares que solicita la IOFE para estos medios, por esa razón realiza la validación también de la confiabilidad del certificado y que sea reconocida con la IOFE, así como el estado de revocación y la vigencia del mismo. Toda plataforma de Intermediación cuenta con un proceso de verificación y validación de las firmas y sellos de tiempo aplicados, determinando que son íntegros.

El sistema verifica que el certificado que se emite sea por una Entidad de Certificación reconocida por la IOFE, por lo cual no permite que se realicen firmas o validaciones en la plataforma, adicionalmente a ello la plataforma tiene políticas adicionales que permiten no solo ver si ha sido reconocida, sino también su fecha de vencimiento o alguna restricción para realizar acciones, tales como estado de revoación, así como verificación con la CRL.

El sistema verifica y valida el certificado del usuario final con la intención de cumplir con el propósito del cifrado o cifrado de clave. Conforme a la RFC 5280.

El sistema descifra la información a través de un algoritmo que se conecta con el módulo criptográfico y que dependa exclusivamente de la llave privada colocada por el usuario o suscriptor. No realizamos copias fuera del módulo criptográfico.

El sistema está desarrollado utilizando tecnologías de información de última generación y herramientas de Intranet e Internet, lo cual permite que usuarios a distancia se integren al sistema en tiempo real. Esta característica es particularmente importante en entidades que tienen oficinas u órganos descentralizados o desconcentrados ya que elimina las distancias físicas, permitiendo el máximo de eficiencia en la gestión documentaria.

Esta propuesta incluye, además, la puesta a disposición de un sistema de comunicación y notificación, firma de documentos, generación de evidencias electrónicas, etc. que facilite y propicie el uso de certificados digitales, todo en armonía a la Ley 27269 “Ley de Firmas y Certificados Digitales”.

Sin embargo, el uso del documento electrónico requiere del mecanismo tecnológico que permite identificar al firmante cuando realice su trámite a través del Sistema Administrativo Interno, para ello los Certificados y Firma Digital resulta vital para establecer una protección técnica, efectiva y que cumpla con las condiciones del marco jurídico peruano.

PROCESOS:

El Sistema Plussigner cubre los siguientes procesos:

a) **Generación y Registro de Documentos o Archivos Electrónicos:** en cada área interna de la empresa, almacenando la información en una base de datos única y con acceso solo del usuario o los usuarios autorizado.
b) **Gestión de los documentos o archivos electrónicos adjuntados por terceros**, al ser ingresados al sistema Plussigner y se generará un código de flujo, para que el usuario de manera lógica a través de un medio de acceso a la red con solo ingresar su número de Trámite pueda visualizar el trámite del expediente y el ver el recorrido que tiene su documento a la fecha.
c) **Gestión de los documentos internos**, entre dependencias o áreas internas de la entidad, existirá un control y un seguimiento detallado y estricto de todos los expedientes que se procesan en la Institución.

FUNCIONES

La plataforma Plussigner tiene las siguientes funciones:

- Registro automático de los documentos emitidos y recibidos, tanto internos como de terceros. Para el cual almacena todos los Registros en una base de datos.
- Creación de Formatos a través de la plataforma y gestión de proceso de la generación masiva a través de servicios o un documento como Excel, csv.
- Derivación automático del tránsito de los documentos entre las dependencias de la entidad.
- Control automático del tiempo de permanencia de cada documento en cada dependencia de la entidad.
- Trazabilidad de los documentos desde la recepción hasta el envío.

La plataforma Plussigner permite, además, las siguientes funciones:

- Predefinir en el sistema la ruta de cada tipo de documento.
- El tiempo máximo de permanencia de cada tipo de documento en cada dependencia.
- La emisión automática de avisos de vencimiento de plazos para los documentos electrónicos.
- Realizar notificaciones electrónicas o alertas electrónicas en cada uno de los procesos de gestión que se desean realizar, esto es configurable por flujo de proceso, los cuales las modalidades son: SMS, Videollamada, Notificación Push, Correo Electrónico .

CONSULTAS Y REPORTES

La plataforma Plussigner permite realizar las siguientes consultas y reportes en tiempo real:

- Estado de trámite de cualquier documento (Ruta de seguimiento, acción de derivación, persona responsable del documento, estado actual del documento o archivo electrónico).
- Visualización de cualquier documento o archivo.
- Visualización de las observaciones y/o anotaciones que va teniendo el documento o archivo
- Reportes de Gestión de Documentos de cada dependencia (Documentos generados, documentos tramitados, documentos en proceso).
- Reportes configurables según los datos que se tengan en la plataforma.

SEGURIDAD

Asimismo, el Plussigner cuenta con los mecanismos más avanzados para garantizar la seguridad e inviolabilidad de los documentos. El acceso a la base de datos y a las diferentes funciones del Sistema está restringido por un sistema de control que autoriza el acceso según niveles y por usuarios, impidiendo el acceso no autorizado y la manipulación de los documentos generados. Esto asegura el transporte desde la generación hasta el envío de la plataforma.

BENEFICIOS

- El Sistema permite interactuar con dependencias ubicadas físicamente en otros lugares facilitando al máximo la comunicación y coordinación entre dependencias u organismos relacionados con la entidad, esta interacción se realiza por internet.
- El Sistema permite mejorar la eficiencia de la gestión administrativa de cada dependencia al proporcionar información objetiva de la gestión documentaria de cada una de ellas y haciendo uso de la Firma Digital.
- Máxima seguridad del archivo documentario y registro permanente e inviolable de todo el trámite documentario.
- Por todo lo anterior la plataforma Plussigner permite racionalizar el uso de los recursos humanos y racionalizar los procedimientos administrativos, logrando con ello un ahorro sustancial para la empresa y sobre todo no se perderán más los expedientes y se dará un mejor servicio a los clientes, y usuarios de la entidad.

CARACTERISTICAS:

- Alta Escalabilidad
- Carga de Datos flexible y con múltiples métodos
- Administración de los documentos o archivos electrónicos salientes completa, amistosa y fácil

- Monitor de Emisión que controla el flujo de documentos o archivos electrónicos salientes.
- Impresión de documentos o archivos electrónicos de pago flexible, configurable y variable
- Configuración de Envío de Títulos Electrónicos a las personas correspondientes.
- Trazabilidad de Recepción que controla el flujo de Títulos Electrónicos.
- Seguridad de Encriptación de Plataforma – SHA 256.

VENTAJAS:

- Plena disponibilidad del Documento Electrónico, en cualquier momento y desde cualquier lugar del mundo. Tan sólo es necesario un punto de acceso a Internet.
- Ahorro económico frente a compulsas o validaciones legales
- Garantía de re-emisión frente a pérdida de título físico.
- Posibilidad de realizar trámites a distancia frente a administraciones o empresas, en los que haya que presentar garantía de titulación.
- Concurrencia en los procesos de selección con el Documento Electrónico, como documento acreditativo y con plena validez legal sobre tu titulación.
- Plena movilidad: máxima facilidad en la acreditación de titulación para la realización de másteres, becas, empleo, etc.
- Ahorro en costos, se estima que el costo promedio por la emisión de documento o archivo electrónico se reduce en 30% por documento emitido.
- Ahorro en tiempo, al evitar la impresión y envió.
- Permite enviar en forma electrónica el documento o archivo electrónico a los involucrados.
- Permite la configuración de los documentos o archivos electrónicos según el formato del cliente.
- Las organizaciones adscritas a este servicio disponen de un sistema automatizado y seguro para la gestión de los títulos que supondrá un ahorro considerable de tiempo y costes en labores administrativas.

ARQUITECTURA

La arquitectura esta especificada en el documento “Diseño de Solución de Arquitectura de Plussigner”, el cual específica a detalle la arquitectura de solución, así como los procesos donde se van a implementar.

10. CERTIFICACIÓN ISO 27001

SI APLICA, como servicio tenemos al proveedor Amazon Web Services que brindan las características mínimas de la ISO 27001 (Anexo Certificación ISO 27001).

AWS administra la seguridad constantemente de forma exhaustiva e integral. Esta norma de seguridad internacional ampliamente reconocida especifica entidades:

- Evaluar sistemáticamente los riesgos de seguridad de la información, teniendo en cuenta el impacto de las amenazas y vulnerabilidades a las que se enfrenta la empresa
- Diseñar e implementar una completa suite de controles de seguridad de la información y otros mecanismos de administración del riesgo para afrontar los riesgos de seguridad de la empresa y la arquitectura
- Adoptar un proceso general de administración para garantizar que los controles de seguridad de la información cumplan nuestras necesidades de seguridad de la información de forma continua

La implementación y la alineación de AWS con las normas ISO 27001, 27017 y 27018 demuestran un compromiso con la seguridad de la información en todos los niveles de la organización. Un auditor externo independiente evalúa a AWS para validar la alineación con la norma ISO 27001. El cumplimento de este código de conducta y normas reconocidas internacionalmente demuestra que el programa de seguridad de AWS es exhaustivo y cumple las prácticas recomendadas más importantes de la industria.

En el caso de OVH ha obtenido la certificación ISO 27001:2013 para sus soluciones Dedicated Cloud. Esta norma controla la existencia de mecanismos de gestión de la seguridad.

11. RESPONSABILIDADES

SOLUCIONES APLICADAS EN TECNOLOGÍA AVANZADA S.A.C exige a sus proveedores la implementación de los controles de seguridad y privacidad necesarios para proteger la información de sus clientes, conforme a lo declarado en el presente documento.

El detalle de las limitaciones de responsabilidad son definidas en los respectivos contratos, según la normatividad y acuerdos con cada cliente.

12. ORGANIZACIÓN QUE ADMINISTRA LOS DOCUMENTOS NORMATIVOS

SOLUCIONES APLICADAS EN TECNOLOGIA AVANZADA S.A.C administra los documentos de Declaración de Prácticas, y todos los documentos normativos del SVA.

Para cualquier consulta contactar:

Nombre: José Junior Damian Tirado

Puesto: Sub Gerente General

Teléfono: +511979668777

Correo: jose.damian@saeta.pe

13. PUBLICACIÓN DE LA DECLARACIÓN DE PRÁCTICAS

La Declaración de Prácticas de Servicios de Valor Añadido de PLUSSIGNER, la Política y Plan de Privacidad y otra documentación relevante son publicados en la siguiente dirección:.

www.saeta.pe/certificados-digitales/practicas-y-politicas-de-sva

Todas las modificaciones relevantes serán comunicadas al INDECOPI y las nuevas versiones del documento serán publicadas en el mismo sitio web.

El presente documento es firmado por el Responsable del SVA antes de ser publicado, y se controlan las versiones del mismo, a fin de evitar modificaciones y suplantaciones no autorizadas. Las versiones cambian conforme son presentadas y aprobadas por el INDECOPI.

14. CONTROLES EN LAS INSTALACIONES, GESTION Y OPERACIONALES

14.1. CUMPLIMIENTO

El cumplimiento de todos los controles en las instalaciones, gestión y operacionales van acorde a la gestión general de la política de seguridad de la información.

14.2. EVALUACIÓN DE RIESGOS

La evaluación de riesgos se contempla en el documento “Gestión y Administración de Riesgos” que tiene la organización.

14.3. CONTROL DE ACCESO A LOS AMBIENTES

El control de acceso a los ambientes, se evidencia en el documento “Política de Seguridad de la Información” que tiene la organización.

14.4. CONTROL DE ACCESOS ACCESO DE USUARIOS

El control de acceso de usuarios, se evidencia en el documento “Política de Seguridad de la Información” que tiene la organización.

14.5. AUTORIZACIÓN PARA RETIRAR EQUIPOS O SISTEMAS FUERA DEL LOCAL

El control de accesos de inventario, se evidencia en el documento “Política de Seguridad de la Información” que tiene la organización.

14.6. GESTIÓN DE ACTIVOS

La gestión de activos, se evidencia en el documento “Política de Seguridad de la Información.

14.7. SEGURIDAD DE LOS RECURSOS HUMANOS

La seguridad de los recursos Humanos, se evidencia en el documento “Política de Seguridad de la Información.

14.8. GESTIÓN DE INCIDENTES

La gestión de Incidentes, se evidencia en el documento “Política de Seguridad de la Información.

14.9. SEGURIDAD DE LA INFORMACIÓN – ANTIVIRUS/SOFTWARE MALICIOSO

La seguridad de la información – Antivirus / Software Malicioso, se evidencia en el documento “Política de Seguridad de la Información

15. NOTIFICACIONES Y COMUNICACIONES ENTRE PARTICIPANTES

Los mecanismos de comunicación con nuestros clientes se realizan a través de nuestra plataforma de gestión, tal cual se realiza al contacto del que administra el documento, esto se realiza a través de:

- Correo firmado digitalmente por el cliente.
- Atención por ticket de ayuda en nuestra plataforma de atención http://saeta.pe/soporte/

Todas las comunicaciones son declaradas al cliente y puestas en la modalidad de contrato o acuerdo con el mismo.

16. POLÍTICA DE REEMBOLSO

Las condiciones de reembolso serán definidas con cada cliente en los respectivos contratos, de acuerdo al tipo de servicio, contrato y cliente. Bajo la póliza de seguro que entra en vigencia el día 19/04/2019 al 19/04/2020 con el número 230182878, donde la aseguradora La Positiva Seguros Perú S.A. emite una póliza de responsabilidad civil para servicios de tecnología, según las condiciones particulares.

17. RESPONSABILIDAD FINANCIERA, REPRESENTACIONES Y GARANTÍAS

Las condiciones de financiera, así como las garantías y representaciones serán definidas con cada cliente en los respectivos contratos, de acuerdo al tipo de servicio, contrato y cliente, las cuales regirán bajo la póliza de seguro que entra en vigencia el día 19/04/2020 al 19/04/2021 con el número 230182878, donde la aseguradora La Positiva Seguros Perú S.A. emite una póliza de responsabilidad civil para servicios de tecnología, según las condiciones particulares.

18. FINALIZACIÓN DEL CONTRATO CON EL SUSCRIPTOR

Una vez finalizado el contrato con el suscriptor, al cual se le entrega una serie de documentos y archivos, los cuales son los siguientes:

- El suscriptor recibirá los documentos generados y firmados por la plataforma en un medio magnético o medio físico según sea el contrato.
- El suscriptor recibirá toda la trazabilidad e historia de cada uno de los documentos generados, en archivo de texto plano o en un archivo de base de datos, según sea el caso de su contratación.
- El suscriptor recibirá un documento de arquitectura e instrucción para poder visualizar los documentos electrónicos.
- El suscriptor recibirá unas credenciales de acceso por un lapso de un mes una vez finalizado el Contrato.

19. ENMENDADURAS

Los procedimientos para la resolución de enmendaduras podrán ser definidas en los contratos con las organizaciones clientes, de acuerdo al tipo de servicio, contrato y cliente.

20. RESOLUCIÓN DE DISPUTAS

Los procedimientos para la resolución de disputas podrán ser definidas en los contratos con las organizaciones clientes, de acuerdo al tipo de servicio, contrato y cliente.

21. ACUERDO ÍNTEGRO, SUBROGACIÓN Y DIVISIBILIDAD

Las cláusulas de acuerdo íntegro, subrogación y divisibilidad podrán ser definidas en los contratos con las organizaciones clientes, de acuerdo al tipo de servicio, contrato y cliente.

22. FUERZA MAYOR Y OTRAS PROVISIONES

Las cláusulas de fuerza mayor y otras provisiones aplicables a la entrega de los servicios de valor añadido podrán ser definidas en los contratos con las organizaciones clientes, de acuerdo al tipo de servicio, contrato y cliente.

23. TARIFAS

Las tarifas por los servicios serán definidas en los contratos con las organizaciones clientes, de acuerdo al tipo de servicio, contrato y cliente, también disponibles en las cotizaciones realizadas.

24. FINALIZACIÓN DEL SVA

Antes de que el SVA termine sus servicios realizará las siguientes medidas:

- De ser aplicable, con 30 días de anticipación se informará a todos clientes y suscriptores, la finalización de las operaciones del SVA.
- Se pondrá a disponibilidad de todas las organizaciones cliente la información concerniente a su terminación y las limitaciones de responsabilidad.
- Se concluirán los permisos de autorización de funciones de todos los subcontratados para actuar en nombre del SVA

- Se mantendrán o transferirán a los terceros que confían sus obligaciones de verificar los documentos generados.
- Las provisiones sobre término y terminación, así como las cláusulas de supervivencia serán definidas en los contratos de los clientes. Además, las modificaciones realizadas deben ser comunicadas a los suscriptores, titulares y terceros que confían.

25. CONFORMIDAD CON LA LEY APLICABLE

SOLUCIONES APLICADAS EN TECNOLOGÍA AVANZADA es afecta y cumple con las obligaciones establecidas por la IOFE, a los requerimientos de la Guía de Acreditación de Entidades Prestadoras de Servicios de Valor Añadido, al Reglamento de la Ley de Certificados Digitales, y a la Ley de Firmas y Certificados Digitales -Ley27269, para el reconocimiento legal de los servicios de valor añadido emitidos bajo las directrices definidas en el presente documento.

26. BIBLIOGRAFÍA

a) Guía de Acreditación de Prestadores de Servicios de Valor Añadido, INDECOPI
b) Ley de Firmas y Certificados Digitales –Ley 27269
c) Decreto Supremo 052-2008
d) Decreto Supremo 070-2011
e) Decreto Supremo 105-2012