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

PLAN DE PRIVACIDAD

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 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.

INFORMACION DE COMO ESTOY PROTEGIENDO, ESTAMOS OBTENIENDO, COOKIES, RESPONSABILIDAD DE DOCUMENTOS INTERNOS.

LISTA DE RIESGOS A NIVEL DE PRODUCTO.

1. ALCANCE

La presente política es de cumplimiento obligatorio para el personal contratado por SOLUCIONES APLICADAS EN TECNOLOGIA AVANZADA S.A.C que participan de las operaciones críticas de los servicios de registro descritos en la Declaración de Prácticas de Registro.

2. INFORMACIÓN RECOLECTADA Y PROTEGIDA

Como parte de las operaciones de registro, Salmon Corp en calidad de SVA de Intermediación electrónica recolecta información de los suscriptores y titulares del siguiente tipo:

- Datos de identificación personal.
- Contrato de solicitud de servicios.
- Documentos o Archivos Digitales.

3. TRATAMIENTO DE LOS DATOS PERSONALES

Deberá considerarse como información no privada, la siguiente:

- Información personal públicamente disponible

En estos casos no será requerida autorización del usuario para dar publicidad a esta información. Deberá considerarse como información privada, la siguiente:

- De conformidad con lo establecido por la Norma Marco sobre privacidad del APEC, se considera información personal, cualquier información relativa a un individuo identificado o identificable.
- Información que pueda permitir a personas no autorizadas la construcción de un perfil de las actividades de los usuarios de los servicios de sellado de tiempo.
- En todos los casos, figurará en la Política de Privacidad que deberá ser suscrita por el mismo, su consentimiento para el tratamiento y almacenamiento de estos datos.

La información personal considerada como privada únicamente será divulgada en caso que exista consentimiento previo y por escrito firmado para tales efectos por el titular de dicha información o medie una orden judicial o administrativa que así lo determine.

Cualquier violación a la privacidad de esta información por parte del personal de la SIE de SAETA o de los terceros subcontratados, será sujeto de sanción.

4. FLUJO TRANSFRONTERIZO DE DATOS PERSONALES

Los contratos de los suscriptores contendrán cláusulas que soliciten el consentimiento del suscriptor y titular de transferir los datos personales contenidos en el certificado digital a los países donde se encuentren las entidades de certificación.

5. IMPLEMENTACIÓN DE LOS PRINCIPIOS DE PRIVACIDAD

El presente documento adopta lo establecido por el APEC a través de la Norma Marco sobre Privacidad respecto de los principios que deben ser observados siempre que se realice algún tipo de labor o función que involucre la recolección, posesión, procesamiento, uso, transferencia o revelación de información personal.

A. Medidas preventivas:

a. Se restringirá el acceso a los datos personales a las personas que implementen la solución de intermediación.

b. Estos datos serán protegidos contra acceso no autorizado.

c. Se concientizar al personal para no divulgar o exponer de manera accidental datos personales de los usuarios

d. Se implementarán procedimientos para documentar las prácticas en lo que respecta a la información personal que se recolecta durante las actividades de operación o comercialización de los servicios de sellado de tiempo, las mismas que deben informar sobre:

i. El hecho de que se está recolectando información personal;

ii. Los propósitos para los cuales se recolecta dicha información personal;

iii. Los tipos de personas u organizaciones a las que dicha información podría ser revelada;

iv. La identidad y ubicación del responsable de la información personal, incluyendo información respecto a la forma de contactarlo en razón a sus prácticas y manejo de la información personal;

v. Las opciones y medios que ofrece el responsable de la información personal a los individuos para limitar el uso y revelación, así como los mecanismos para el acceso y corrección de su información.

vi. Deben tomarse todos los pasos razonablemente necesarios, a fin de asegurar que se provee tal información, sea antes o en el mismo momento en que se está efectuando la recolección de la información personal. Caso contrario, deberá proveerse esta información tan pronto como sea factible.

e. Puede no resultar apropiado exigir que los responsables de la información personal provean información respecto a la recolección y uso de información que se encuentra públicamente disponible.

B. Uso de la información personal

a. La información personal recolectada será usada en estricto cumplimiento de los propósitos de la recolección o aspectos relativos a los mismos, excepto:

1. Que exista consentimiento del individuo al que pertenece la información personal recolectada;

2. Que esta información fuera necesaria para la provisión de un servicio o producto solicitado por el individuo; o

3. Que la recolección fuera permitida por mandato de ley u otros instrumentos legales o exista algún tipo de pronunciamiento con efectos legales que lo autorizara.

C. Elección

a. Cuando sea apropiado, se proveerá a los individuos mecanismos claros, prominentes, fáciles de entender, accesibles y económicos a fin que puedan decidir respecto a la recolección, uso y revelación de su información personal. Puede no resultar necesario que los responsables de la información provean estos mecanismos en los casos de recolección de información que sea públicamente disponible.

D. Integridad de la información personal

a. La información personal deberá ser exacta, completa y mantenerse actualizada en el extremo que fuere necesario para los propósitos de su empleo.

E. Salvaguardas a la seguridad

a. Los responsables de la información personal deberán proteger la información personal que mantienen, a través de salvaguardas apropiadas contra riesgos tales como pérdida de la información o acceso indebido a la misma, así como contra la destrucción, uso, modificación o revelación no autorizada o cualquier otro abuso. Estas salvaguardas deberán ser proporcionales a la naturaleza y gravedad del daño potencial, la sensibilidad de la información y el contexto en que ésta es mantenida, y deberán ser sometidas a revisiones y reevaluaciones periódicas.

F. Acceso y corrección

a. Los individuos deben ser capaces de:

1. Obtener del responsable de la información personal, la confirmación respecto a si mantiene o no información personal que les concierne.

2. Comunicar su información personal, luego de haber probado suficientemente su identidad, dentro de un periodo de tiempo razonable; por una tarifa, si es que la hubiera, la cual no debe ser excesiva; de una manera razonable; de un formato que sea razonablemente comprensible; y

3. Cuestionar la exactitud de la información que les concierne y de ser posible y apropiado, hacer que la información sea rectificada, completada, enmendada o borrada.

b. Debe proveerse acceso y oportunidad para la corrección de la información, salvo cuando:

1. La carga o costo de hacerlo sea indebido o desproporcional a los riesgos de la privacidad individual en el caso en cuestión;

2. La información no pueda ser divulgada por razones legales o de seguridad o para proteger información comercial de carácter confidencial; o

3. Se podría violar la privacidad de la información de personas diferentes al individuo.

Si una solicitud bajo el supuesto (a) o (b) o un cuestionamiento bajo el supuesto (c) es denegado, se debe informar al individuo las razones en las que se basa dicha denegatoria y se le debe informar respecto a los mecanismos para cuestionar dicha decisión.

6. RESPONSABILIDADES

El Responsable de Privacidad gestiona la implementación y vela por el cumplimiento de la presente política así como de su revisión periódica, actualización, difusión y concientización y capacitación al personal y terceros para su adecuado cumplimiento.

7. CONFORMIDAD

Este documento ha sido aprobado por el Responsable de SOLUCIONES APLICADAS EN TECNOLOGÍA AVANZADA en calidad de SVA intermediación electrónica, y cualquier incumplimiento por parte de los empleados, contratistas y terceros mencionados en el alcance de este documento, será comunicado a dicha autoridad para la ejecución de las sanciones respectivas.