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

POLITICA 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.

El cómo voy a cuidar los procesos de privacidad.

Considerar el siguiente dominio:

Sie.plussigner.com

POLÍTICA DE PRIVACIDAD

1. ALCANCE

La presente política es de obligatorio cumplimiento para todos los empleados y proveedores de SOLUCIONES APLICADAS EN TECNOLOGIA AVANZADAS S.A.C. que tienen relación con los servicios de sellado de tiempo.

2. POLÍTICA DE PRIVACIDAD DE DATOS PERSONALES

SOLUCIONES APLICADAS EN TECNOLOGIA AVANZADAS S.A.C. no recogen información personal de los usuarios (personas naturales) de los servicios de sellado de tiempo, ya que estas transacciones no implican firma digital del usuario final.

3. CUMPLIMIENTO DE REQUERIMIENTOS LEGALES

SOLUCIONES APLICADAS EN TECNOLOGIA AVANZADAS S.A.C. como Autoridad emisora de intermediación Electrónica, cumple los requerimientos establecidos en la Guía de Acreditación de Entidades Prestadoras de Servicios de Valor Añadido, el Reglamento y la Ley de Firmas y Certificados Digitales -Ley27269.

4. CONFORMIDAD

Este documento ha sido aprobado por la Autoridad de la SIE en SOLUCIONES APLICADAS EN TECNOLOGIA AVANZADAS S.A.C., y tiene carácter normativo sobre todos los servicios de sellado de tiempo, por lo que cualquier incumplimiento por parte de las personas mencionadas en el alcance de este documento, será comunicado a dicha autoridad para la ejecución de las sanciones respectivas.

(COMO GARANTIZAR EL MANEJO Y LA PRIVACIDAD DEL DOCUMENTO) INCLUIR UN CONSENTIMIENTO CON EL USUARIO DEL MANEJO DE LA INFORMACIÓN.