INSTITUTO MIXTO DE AYUDA SOCIAL
GERENCIA GENERAL
ÁREA TECNOLOGÍAS DE INFORMACIÓN

Política de Seguridad de la información

POL-TI-08

Junio, 2017

ÍNDICE

1. JUSTIFICACIÓN

Es necesario contar con lineamientos que, mediante el uso de mecanismos de seguridad digital, se anticipen y eviten que la información institucional sea vulnerable a ataques tanto desde fuentes externas (entiéndase como delincuentes digitales: sean personas físicas o delincuencia automatizada) como de personas no autorizadas para acceso a la información, de forma que se proteja y salvaguarde en todo momento la información institucional.

2. DEFINICIONES

Conciencia de Seguridad: la medida en que una organización está comprometida con la aplicación de las mejores prácticas a nivel de seguridad y las implicaciones de no hacerlo.

Incidentes: cualquier evento que no es parte de una operación estándar de un servicio y que causa, o puede causar, una interrupción del servicio, o una reducción en la calidad del mismo.

Vulnerabilidad: la medida en la que se verá afectado un componente o un servicio por una amenaza.

Información: conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje. Para esta Política entiéndase información la proveniente de sistemas de información social, financiera, administrativa y comercial.

Seguridad de la Información: es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.

Software: componente lógico, programa de computadora o aplicativo de computadora, desarrollado para una función específica o varias funciones según se desarrolle.

Muro de fuego o Firewall: También conocidos como “cortafuegos”, es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Abreviaturas:

TI: Tecnologías de Información.

IMAS: Instituto Mixto de Ayuda Social

3. OBJETIVOS

3.1 Objetivo General:

Proveer una apropiada dirección estratégica que permita mostrar la importancia de la seguridad de la información en los procesos de la Institución.

3.2 Objetivos Específicos:

- Proteger la información institucional, mediante el manejo adecuado de la seguridad de la información utilizando los mecanismos adecuados.
- Promover la cultura y actitudes necesarias para mantener un estado óptimo sobre la seguridad de la información de los procesos institucionales realizados por las personas funcionarias.

4. FUNDAMENTO LEGAL

Normas técnicas de la Contraloría General de la República para Tecnologías de Información.

Documentación relacionada:

P-TI-29 Procedimiento para la Administración de Seguridad en los Sistemas

5. ÁMBITO DE APLICACIÓN

5.1 Alcance:

Esta política resulta aplicable a todas las personas funcionarias y trabajadoras del IMAS, asimismo, contratistas o terceras personas que tengan acceso a los sistemas de información de la Institución.

5.2 Responsabilidades:

- Es responsabilidad del Comité Gerencial de Tecnologías de Información y del Área Tecnologías de Información velar por la Seguridad de la Información del IMAS.

- Supervisión: es responsabilidad de la Gerencia General supervisar, al menos una vez al año, el cumplimiento de esta política, para lo cual se puede apoyar asignando una persona funcionaria de dicha gerencia, a fin de que supervise mediante los mecanismos de verificación.

- Mecanismos de verificación: son mecanismos de verificación de esta política los siguientes:

  - Informes de necesidades de concientización o capacitación que TI remite a la Gerencia General o a Desarrollo Humano en forma anual.
  - Reportes de incidentes de seguridad reportados vía sistema tiquetes, correo electrónico u oficio formal, a los cuales TI deberá dársele un tratamiento especial prioritario y seguimiento hasta el cierre de la solución.
  - Solicitudes para emisión de directrices emitidas por TI hacia la Gerencia General en materia atinente.
  - Análisis de vulnerabilidades de la red.
  - Adquisición, renovación e instalación de licenciamientos para antivirus y de software de protección de perímetro (muro de fuego/firewall).
  - Contratos de confidencialidad con funcionarios que tienen acceso a sistemas de información, así como de los contratos de confidencialidad con terceros que tienen acceso a los sistemas o a la información institucional a través de convenios u otros accesos autorizados.

- Seguimiento:

  La Gerencia General deberá establecer planes de acción y medidas correctivas cuando detecte incumplimiento de esta política. Así mismo brindar el seguimiento a dichos planes de acción y medidas correctivas.

5.3 Penalidades:

El incumplimiento de esta política por parte de una persona funcionaria o trabajadora, será notificado al Área de Desarrollo Humano, por el Área de Tecnologías de Información, cuando ésta sea notificada o haya detectado alguna anomalía o incumplimiento, y será el Área de Desarrollo Humano quien debe acatar lo dispuesto en el Reglamento Autónomo de Servicios. Corresponde a la Gerencia General del IMAS, previa elaboración del procedimiento administrativo correspondiente, instruir al Área de Desarrollo Humano para que se apliquen las sanciones correspondientes.

6. DISPOSICIONES GENERALES DE LA POLÍTICA

Es responsabilidad del Área de Tecnologías de Información establecer directrices para la gestión de la Seguridad de la Información del IMAS.

El Área de Tecnologías de Información debe asegurar que los objetivos y estrategias de la Seguridad de la Información del IMAS se encuentren alineados con los objetivos institucionales.

El Área de Tecnologías de Información debe promover la implementación de las normas de seguridad necesarias de acuerdo con las tecnologías en uso, contando con el apoyo de las áreas involucradas.

El Área de Tecnologías de Información debe identificar y recomendar a la Gerencia General, las necesidades de concienciación y capacitación del personal del IMAS en temas de Seguridad de la Información. En caso de algún problema de seguridad en el resguardo de la información se deberá informar de manera célere y oportuna a la Gerencia General.

El Área de Tecnologías de Información debe definir en forma conjunta con el área de Desarrollo Humano las campañas de capacitación en los temas identificados.

El Área de Tecnologías de Información debe monitorear y estar alerta acerca de los incidentes de seguridad de la información y dar el seguimiento necesario para su solución.

El Área de Tecnologías de Información debe gestionar la elaboración del análisis de vulnerabilidades y riesgos en la plataforma tecnológica, así como, la realización de evaluaciones externas cuando lo considere oportuno sobre la misma.

El Área de Tecnologías de Información deberá de proveer de las herramientas necesarias para la protección de la información Institucional; como software de antivirus, software de seguridad de perímetro.

Las computadoras utilizadas por las personas funcionarias de la Institución y que están conectadas a las redes del IMAS, sean o no propiedad del empleado o de la Institución, deben continuamente ejecutar un “software” o programa antivirus actualizado, caso contrario no deberán conectarse a la red.

Las personas funcionarias o personas usuarias deben ser extremadamente cautelosas en el momento de recibir un correo electrónico con adjuntos de remitentes desconocidos, los cuales pueden contener virus, correo bombas, código de caballos troyanos, entre otros; con el objetivo de no poner en riesgo la seguridad digital institucional.

Todas las personas funcionarias del IMAS, terceros y personas usuarias de los activos de información, deben utilizar dichos recursos de acuerdo con los derechos y responsabilidades que se les asignen de conformidad con sus funciones, así como, conocer y cumplir las regulaciones en materia de Seguridad de la Información. Estos tienen la responsabilidad de reportar a la jefatura inmediata cualquier caso sospechoso que atente contra la Seguridad de la Información del IMAS.

De presentarse algún caso sospechoso que atente contra la Seguridad de la Información de los activos de información del IMAS, la jefatura inmediata que recibe el reporte debe remitirlo al Área de Tecnologías de Información.

El Área de Tecnologías de Información debe promover la asociación e integración con grupos especialistas en temas de seguridad, así como, también establecer la coordinación con apropiadas autoridades que fortalezcan la gestión de Seguridad de la Información.

En cuanto a temas de resguardo de la información se deberá seguir lo estipulado en la Ley 8968 “Ley de Protección de las Personas Frente al Tratamiento de sus Datos Personales”

7. UNIDAD FORMULADORA

La Unidad Formuladora de esta política es el Área de Tecnologías de Información.

8. REVISIÓN Y ACTUALIZACIÓN

El Consejo Directivo será responsable de la aprobación de este documento.

La revisión y cambios a realizar en esta política es responsabilidad de la persona que ocupe el cargo de jefatura del Área de Tecnologías de Información.

Los documentos serán revisados cuando por cambios del funcionamiento del área de TI sea requerido, incorporando los cambios y actualizaciones para adaptarlo a las necesidades.

El Centro de Documentación y Recursos (CIRE) es el responsable de mantener en custodia los documentos de normativa aprobados.