PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

VIGENCIA 2018

INTRODUCCIÓN

Todos los equipos que componen el Sistema de Información manejado por los funcionarios de la ESE Hospital San Vicente de Paul de Mistrató, al igual que los diferentes bienes y procesos, están expuestos a diferentes riesgos, que pueden derivar en problemas significativos que afecten el cumplimiento de los objetivos misionales. Por este motivo, el Hospital realiza un plan que busca mantener segura tanto la información requerida para su funcionamiento, como la información privada que el Hospital maneja de sus usuarios.

OBJETIVO GENERAL

Garantizar un nivel razonable de seguridad y respaldo del sistema de información de la ESE Hospital San Vicente de Paul de Mistrató, teniendo en cuenta todos los tipos de software que se manejan en la institución.

OBJETIVOS ESPECÍFICOS

- Capacitar a todos los funcionarios de la ESE con acceso a sus sistemas de información, en el manejo de las herramientas tecnológicas para minimizar el riesgo de pérdida de información de cualquier índole.

- Implementar las políticas de buen manejo y seguridad de la información existentes desde el área de gestión de calidad.

ALCANCE

La Política de Seguridad de la Información aplica a todos las partes interesadas en todos los niveles jerárquicos, proveedores y terceros, que produzcan, administren, custodien o que tengan acceso a la información.

La red del Hospital cuenta con tecnologías de información suficientes: sistema de comunicación interno para realizar llamadas entre dependencias, intranet para la comunicación entre funcionarios, software contable, software de facturación, software de presupuesto y nómina, software de costos, software para el manejo de historias clínicas.

SEGURIDAD DE INFORMACIÓN Y PROTECCIÓN DE DATOS

Cuando hablamos de seguridad informática dentro de una institución como la ESE Hospital San Vicente de Paul de Mistrató, debemos distinguir dos propósitos de protección, y es vital distinguirlos ya que forman la base, dan la razón y justificación en la selección de los elementos de información que requieren una atención especial dentro del marco de la Seguridad de la Información y normalmente dan el motivo para su protección. Los dos propósitos son la seguridad de la información y la protección de datos. A pesar de que hay diferencia entre seguridad de la información y la protección de datos, las medidas de protección aplicadas normalmente serán las mismas.

El objetivo principal de la seguridad de la información es la protección de los datos internos de funcionamiento y tratar de evitar la pérdida o modificación no autorizada. La protección de datos por otro lado, debe garantizar la

confidencialidad, integridad y disponibilidad de datos de los funcionarios y partes interesadas, sin embargo, existen más requisitos como por ejemplo la autenticidad de datos.

La motivación para implementar medidas de protección que responden a la seguridad de la información, responde al interés propio de la ESE, ya que la pérdida o modificación de información relevante, puede generar daños, ya sean materiales o no, los cuales, pueden repercutir de manera directa en la economía del Hospital. Cuando hablamos de protección de datos, el móvil corresponde más a la normatividad y a la necesidad de proteger información privada a la cual solo pueden tener acceso, funcionarios de la ESE con suficiente nivel de autorización o los mismos usuarios dueños de la información (Historias Clínicas).

Para proteger la información es necesario realizar una gestión de riesgos oportuna que permita ejecutar acciones de control que permitan mitigar la posibilidad de ocurrencia de los mismos. La gestión de riesgos debe hacer parte integral de un proceso de mejora continua con los procesos de la Institución y debe incluir a todos los funcionarios.

Teniendo en cuenta lo anterior, para elaborar un plan de seguridad de la información oportuno, se deben tener en cuenta las amenazas y vulnerabilidades. Una amenaza es la posibilidad de ocurrencia de cualquier tipo de evento o acción que pueda generar daño sobre los elementos del sistema de información de la ESE. Debido a que la Seguridad Informática tiene como propósito, garantizar la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones. Desde la perspectiva del Hospital, existen amenazas externas como las agresiones técnicas, de la naturaleza o por parte humano. También existen amenazas internas como la negligencia del personal o la falta de procedimientos de mantenimiento preventivo y correctivo.

Por otra parte, la vulnerabilidad, son las características del sistema, que lo hacen susceptible a amenazas, las cuales pueden tener como consecuencia, la

generación de un daño. Por este motivo los sistemas de información del Hospital, debe tener la capacidad de responder o reaccionar a una amenaza e incluso debe poder recuperarse de un daño generado. Lo anterior mencionado se traduce en gestionar el riesgo.

El primer paso en la gestión del riesgo, es el análisis de riesgo que tiene como propósito determinar los componentes de un sistema que requieren protección, puesto que sus vulnerabilidades pueden exponer el sistema a amenazas que lo pongan en peligro. El análisis debe generar una valoración de grado de riesgo. La gestión del riesgo en la ESE Hospital San Vicente de Paul de Mistrató, se realizará conforme con la Política de Administración del Riesgo implementada desde el sistema de gestión de calidad.

Clasificación y Flujo de Información

Esta actividad tiene como propósito, el garantizar que los datos que componen la información de la ESE sean protegidos. Para lograr el objetivo, se debe clasificar a los funcionarios que manejan los sistemas de información, manejando diferentes niveles de autorización, con el fin de proteger los datos tanto de funcionamiento del Hospital, como los datos administrados de los usuarios. Teniendo en cuenta que estamos hablando de un Hospital, se deben definir niveles de clasificación confidencial, privado, sensitivo y público. De acuerdo a los niveles de clasificación de la información, se definirán los niveles de autorización para los diferentes funcionarios de la Institución, de acuerdo con sus funciones asignadas. Los niveles de autorización en la ESE se definen mediante la creación de usuarios personales cuyos niveles de autorización se restringen mediante una parametrización. Esta actividad mitiga el riesgo de un acceso no autorizado que pueda filtrar información o realizar modificaciones indebidas.

Backups

En términos generales, todas las amenazas que se puedan presentar en el sistema de información de la ESE Hospital San Vicente de Paul de Mistrató, terminan derivando en la pérdida de información relevante o en la utilización en fines para los cuales no debería estar destinada; por este motivo, es primordial para la ESE, la obtención y almacenamiento de copias de seguridad. Para logra este fin, el servidor que contiene la información financiera y las historias clínicas hace copias diarias de seguridad por medio de Freefilesync, enviando la información siempre a un disco duro externo. Los demás terminales son sujetos a mantenimientos periódicos en los cuales se realizan copias de seguridad a los equipos con información administrativa importante. Este mantenimiento se realiza 3 veces al año por medio de un contratista idóneo para realizar esta función.

IVONNE MARITZA ZAPATA CAÑAS
GERENTE