PLAN DE LA POLITICA DE SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

E.S.E HOSPITAL SAN JOSÉ DEL GUAVIARE

2021

TABLA DE CONTENIDO

RESUMEN EJECUTIVO

Mediante la definición del plan de la política de sistema de gestión de la seguridad de la información la E.S.E HOSPITAL SAN JOSÉ DEL GUAVIARE busca mitigar los posibles riesgos derivados del uso de las nuevas tecnologías, esto con el fin de garantizar la seguridad de la información, en aspectos tales como disponibilidad, confiabilidad, accesibilidad e integridad de la misma.

El plan de la política de sistema de gestión de la seguridad de la información se define con el fin de evaluar las posibles acciones que se deben tomar para mitigar los riesgos existentes en los activos de información de la entidad, las cuales son organizadas en forma de medidas de seguridad denominados controles, y para cada una de ellas se define el nombre de la medida, objetivo, justificación, responsable de la medida y su prioridad.

INTRODUCCIÓN

El plan de la política de sistema de gestión de la seguridad de la información en la E.S.E Hospital San José del Guaviare, se basa en una orientación a cada uno de los funcionarios de la institución sobre la importancia de la generación, trasferencia, conservación y uso de la información, por lo cual se debe garantizar el mínimo de riesgo y un alto grado de seguridad que favorezca el desarrollo de la organización, que permita su óptimo funcionamiento y el buen uso de la misma, a través de personas idóneas, capacitadas, procesos implementados y evaluados, backups de seguridad, equipos tecnológicos y de comunicación, permitiendo la recuperación de la información en el menor tiempo posible en caso de incidentes o eventos catastróficos.

El plan de la política de sistema de gestión de la seguridad de la información preserva la confidencialidad, la integridad y la disponibilidad de la información, mediante la aplicación de un proceso de gestión del riesgo, y brinda confianza a las partes interesadas acerca de que los riesgos son gestionados adecuadamente.

DEFINICIONES

Se listan algunos términos y definiciones de términos que se utilizarán durante el desarrollo de la política de sistema de gestión de la seguridad de la información.

La Historia Clínica: Es un documento privado, obligatorio y sometido a reserva, en el cual se registran cronológicamente las condiciones de salud del paciente, los actos médicos y los demás procedimientos ejecutados por el equipo de salud que interviene en su atención. Dicho documento únicamente puede ser conocido por terceros previa autorización del paciente o en los casos previstos por la ley.

Integralidad: La historia clínica debe reunir la información de los aspectos científicos, técnicos y administrativos relativos a la atención en salud en las fases de fomento, promoción de la salud, prevención específica, diagnóstico, tratamiento y rehabilitación de la enfermedad, abordándolo como un todo en sus aspectos biológico, psicológico y social, e interrelacionado con sus dimensiones personal, familiar y comunitaria.

Disponibilidad: Es la posibilidad de utilizar la historia clínica en el momento en que se necesita, con las limitaciones que impone la Ley.

Oportunidad: Es el diligenciamiento de los registros de atención de la historia clínica, simultánea o inmediatamente después de que ocurre la prestación del servicio.

Activos de información: Elementos de Hardware y de Software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. Este tipo de activo representa los datos de la organización, información que tiene valor para los procesos de negocio, independientemente de su ubicación: puede ser un documento físico debidamente firmado, un archivo guardado en un servidor, un aplicativo o cualquier elemento que permita almacenar información valiosa o útil.

Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Control: Es toda actividad o procesos encaminado a mitigar o evitar un riesgo, Incluye políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas que pueden ser de carácter administrativo, técnico o legal.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

Propietario/responsable de activo de información: Individuo, entidad o unidad de negocio que ha aceptado la responsabilidad de la administración para el control, producción, desarrollo, mantenimiento, uso y seguridad de los activos de información.

Servicio: Es cualquier acto o desempeño que una persona puede ofrecer a otra que es esencialmente intangible y que no conlleva ninguna propiedad. Su producción puede o no estar ligada a un producto físico.

Usuario: Es el nombre (o alias) que se le asigna a cada persona para ser identificado por un sistema informático o producto de software, de esta manera el sistema puede diferenciar a cada usuario por medio de sus credenciales (usuario y contraseña) y así mismo relacionar registros de movimientos y permisos de accesos para operar en el mismo.

Amenaza: Evento que puede desencadenar un incidente en la institución, produciendo daños materiales o pérdidas inmateriales en sus activos.

Control de Acceso: Técnica usada para definir el uso de programas o limitar la obtención y almacenamiento de datos a una memoria. Característica o técnica en un sistema de comunicaciones que permite o niega el uso de algunos componentes o algunas de sus funciones.

Cracking: Conducta delictiva en la cual un individuo se infiltra ilegalmente en sistemas informáticos (denominado cracker o pirata informático) y alteran, modifican o eliminan, los datos de un programa o documento informático con la finalidad de obtener un beneficio de dicha alteración.

Hardware: Partes físicas y tangibles de una computadora: sus componentes eléctricos, electrónicos, electromecánicos y mecánicos, sus cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado.

Software: Conjunto de componentes lógicos necesarios que hacen posible la realización de tareas específicas.

Vulnerabilidad: Posibilidad de ocurrencia de la materialización de una amenaza sobre un Activo.

Virus informático: software que tiene como objetivo alterar el funcionamiento normal de cualquier tipo de dispositivo informático, sin el permiso o el conocimiento del usuario para lograr fines maliciosos sobre el dispositivo.

OBJETIVO GENERAL

El plan de la política de sistema de gestión de la seguridad de la información busca proteger los activos de información de la ESE Hospital San José del Guaviare, a través de la estandarización de lineamientos para la implementación de un sistema de gestión de la información, en el cual se establezcan controles para disminuir los riesgos potenciales de perdida de información sensible e importante para la institución, permitiendo satisfacer las necesidades de información y su interrelación con los diferentes clientes.

ALCANCE

Aplica para todos los procesos institucionales, desde la generación de la información hasta el tratamiento, análisis y almacenamiento de la misma.

METODOLOGÍA

El plan de la política de sistema de gestión de la seguridad de la información contempla la definición de las actividades a desarrollar con el objetivo de mitigar los riesgos potenciales de perdida de información sensible e importante para la institución, permitiendo satisfacer las necesidades de información y su interrelación con los diferentes clientes.

ACTIVIDAD	**RESPONSABLE**	**FECHA O PERIODICIDAD**
Socialización de la política de sistema de gestión de la seguridad de la información.	Sistemas de información	Marzo
Identificación de posibles amenazas o vulnerabilidades en la infraestructura tecnológica de la entidad.	Sistemas de información	Todos los días
Implementación de controles y acciones que mitiguen las vulnerabilidades detectadas	Sistemas de información	Al detectar vulnerabilidad
Acciones de concientización a los funcionarios de la institución sobre la importancia de la generación, trasferencia, conservación y uso de la información.	Sistemas de información	Cada mes
Socialización a los funcionarios de la entidad sobre buenas prácticas para garantizar el mínimo de riesgo de la información y un alto grado de seguridad de la misma.	Sistemas de información	Cada mes

RECURSOS

La E.S.E Hospital San José Del Guaviare dispone de la Oficina de Sistemas de información, quién es responsable de coordinar, implementar, modificar y realizar seguimiento a la política de sistema de gestión de la seguridad de la información, lo cual contribuye a la mejora continua.