INTRODUCCIÓN

El Hospital Local De Piedecuesta adopta el plan de tratamiento de riesgos de seguridad de la información como medida para mitigar los riesgos presentes en la institución los cuales se pueden clasificar en secciones como: perdida de la información, perdida de la confidencialidad, integridad y disponibilidad de la misma, evitando de esta manera la realización estratégica del funcionamiento de la entidad.

Este plan define el tratamiento del riesgo con el fin de evaluar las posibles acciones que se deben tomar para mitigar los riesgos existentes, de igual manera establece los lineamientos y respuestas para atender en forma oportuna, ante la posible pérdida, destrucción o robo de la información. Tanto el Hardware como el Software están expuestos a diversos Factores de Riesgo Humano y Físico. Pueden originarse pérdidas de información catastróficas, bien por grandes desastres (incendios, terremotos, sabotaje, etc.) o por fallas técnicas (errores humanos, virus informático, etc.) que pueden producir daño físico irreparable.

Las siguientes medidas se definen teniendo en cuenta la información suministrada mediante el análisis de los riesgos establecidos, y las necesidades del proceso de Gestión de la información y tecnología de la E.S.E Hospital Local De Piedecuesta, en cuanto a la seguridad de la información y proporciona las herramientas necesarias para identificar las medidas de corrección de riesgos y su ejecución en la institución.

1. GENERALIDADES

1.1 Objetivos

1.1.1 Objetivo General

Este plan constituye una estrategia con el propósito de definir y aplicar los lineamientos para tratar de manera integral los riesgos de seguridad digital que el hospital local de Piedecuesta pueda estas expuesto.

1.1.2 Objetivos Específicos

- Evaluar, analizar y prevenir los riesgos informáticos en la E.S.E Hospital Local de Piedecuesta.
- Gestionar riesgos de seguridad y privacidad de la información, de acuerdo con los alcances establecidos en la institución.
- Crear e implementar un enfoque de sistemas para planificar, implementar, monitorizar y gestionar los riesgos de la seguridad de la información.

1.2 Alcance

El Plan de Contingencia Informático está basado en la realidad que manifiesta la E.S.E Hospital Local de Piedecuesta, y puede servir como punto de partida hacia la adecuación y establecimiento de políticas en los diferentes procesos.

2. Responsables

Ingeniero de sistemas

3. Definiciones

AMENAZA: probabilidad de ocurrencia, durante un período específico y dentro de un área determinada, de un fenómeno que puede potencialmente causar daños en los elementos en riesgo.

VULNERABILIDAD: La vulnerabilidad se refiere al grado de pérdidas relacionadas con un elemento en riesgo (o un conjunto de elementos en riesgo), que resulta como consecuencia de un fenómeno natural o artificial con una determinada magnitud. Se expresa de una escala de "0" (no hay daños) a "1" (daño total).

RIESGO: Se refiere a la cuantificación de los posibles daños ocasionados a los elementos en riesgo como consecuencia de un fenómeno natural o artificial en términos de vidas perdidas, personas heridas, daños materiales y ambientales e interrupciones de la actividad económica.

GRAVEDAD: Se refiere a la magnitud resultante de los daños provocados por un siniestro. Esta es subdividida en ninguna, insignificante, marginal, crítica y catastrófica y se definen según el factor de evaluación (víctimas, pérdidas económicas, suspensión de operación, daño ambiental).

SEGURIDAD: Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que, en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados.

DATOS: Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos.

INCIDENTE: Es una violación con éxito de las medidas de seguridad, como el robo de información, el borrado de archivos de datos valiosos, el robo de equipos, PC, etc.

ACTIVO: Son todo aquellos recursos o componentes de la institución, tanto físico (tangibles), como lógicos (intangibles) que constituyen su infraestructura, patrimonio, conocimiento y reputación en el mercado.
CONTROL: Medida que modifica el riesgo

CRITERIOS DEL RIESGO: Termino de referencia frente a los cuales la importancia de un riesgo se evalúa.

EVALUACIÓN DEL RIESGO: Proceso de comparación de los resultados del análisis de riesgo, para evaluar, y determinar su magnitud o si son aceptables o tolerables.

ESTIMACIÓN DEL RIESGO: Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

NIVEL DEL RIESGO: Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la clasificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.

MONITOREO: Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de control o las diferentes auditorias de los sistemas integrados de gestión.

TRATAMIENTO DE RIESGO: Proceso para identificar y modificar el riesgo.

RIESGO DE SEGURIDAD DE INFORMACIÓN: Posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales.

4. POLITICAS DE ADMINISTRACION DE RIESGOS Y ESTRATEGIAS

4.1 Factores

El Hospital Local De Piedecuesta, se compromete a mantener una cultura de gestión de riesgo de la información, con un enfoque basado en el riesgo de seguridad de la información, luchando constantemente con las diferentes circunstancias que puedan alterar el orden de las mismas, mediante mecanismos sistemas y controles enfocados a la prevención y detección de hechos asociados a estas acciones y fortaleciendo las medidas de control u la eficiencia a lo largo del proyecto.

Se deben tener en cuenta alguna de las siguientes opciones, las cuales pueden considerarse independientemente, interrelacionadas o en conjunto.

- **EVITAR:** Es eliminar la probabilidad de que ocurra o disminuir el impacto del riesgo, lo que requiere la eliminación de la fuente del riesgo.
- **PREVENIR:** planear estrategias conducentes a que el evento no ocurra o que se disminuya su probabilidad
- **REDUCIR O MITIGAR:** La protección en el momento en que se presenta el evento, para ello se implementan los planes de emergencia, planes de contingencia entre otros.

- **DISPERSAR:** Dividir una actividad en diferentes componentes operativos de manera que las actividades no se encuentren en un mismo sitio o bajo una sola responsabilidad.

5. METODOLGIA

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos de información de los diferentes procesos del Hospital Local De Piedecuesta, dichas actividades se estructuran de la siguiente manera.

Fase	Actividades	Responsables	Fecha Inicio	Fecha Fin
1. Planeación de la gestión del riesgo	Revisar y ajustar metodología acorde a las necesidades de la institución	Líder de sistemas	Enero 2021	Febrero 2021
2. Identificación y valoración de activos	Identificación. Clasificación y valoración de activos de la institución	Líder de sistemas	Febrero 2021	Abril 2021
3. Identificación de amenazas y vulnerabilidad	Identificar posibles amenazas	Líder de sistemas	Abril 2021	Mayo 2021
4. Análisis del riesgo	De determina la probabilidad de que ocurra el riesgo y el impacto que causaría	Líder de sistemas	Mayo 2021	Junio 2021
5. Desarrollo e implementación de controles	Implementación de los controles y medición.	Líder de sistemas	Agosto 2021	Septiembre 2021
6. Monitoreo y análisis	Se realiza la evaluación y análisis de los riesgos y su potencial impacto	Líder De sistemas	Octubre 2021	Diciembre 2021

6. OPORTUNIDAD DE MEJORA

Los riesgos que se podrán identificar deberán ser monitoreados constantemente, ya que en la actualidad estos mismos se van actualizando periódicamente, además se deberá estar actualizando el recurso tecnológico de la entidad de manera regular siempre y cuando la demanda lo requiera.