E.S.E HOSPITAL SANTA ISABEL GOMEZ PLATA

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD

Responsables:

Gerente E.S.E Hospital Santa Isabel
Administradora de recursos humanos y tecnológicos
Analista de soporte tecnológico

Tabla de contenido

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI – HSIGP

Nombre del documento	HSIGP_Plan_de_desarrollo_informatico
Versión del documento	1.0
Fecha	03/01/2022
Resumen	El presente documento define las medidas de seguridad identificadas para desarrollar e implementar en el transcurso del 2022, el plan de tratamiento para los riesgos de seguridad y privacidad de la información.

Control de cambios		
Fecha	Versión	Descripción
03/01/2022	1.0	Creación

	Fecha	Nombre	Cargo o perfil
Elaborado	03/01/2022	Alex David Zapata Palacio	Contratista, Analista de Soporte
Revisado	10/01/2022	Diana Riveros	Contratista, Talento Humano
Aprobado			

1 RESUMEN EJECUTIVO

Mediante la definición del plan de tratamiento de riesgos se busca mitigar los riesgos y los problemas (perdida de la confidencialidad de la información hospitalaria, perdida de integridad de los registros y perdida de disponibilidad) evitando aquellas situaciones que impidan el logro de los objetivos del Ministerio Tecnologías de la Información y las Comunicaciones (MINTIC).

El plan de tratamiento de riesgo se define con el fin de evaluar las posibles acciones que se deben tomar para mitigar los riesgos existentes, para evitar situaciones que alteren las medidas de seguridad que se requieren implementar, y para cada una de ellas se define el nombre de la medida, objetivo, justificación, responsable de la medida y su prioridad.

Las anteriores medidas se definieron teniendo en cuenta la información los riesgos, y la necesidad de asegurar la calidad de la información con los planes y procesos generados por el Ministerio TIC en cuanto a la seguridad de la información y los problemas ocasionados por el mal manejo de estas, para definir cada una de las características de las medidas y la definición de los pasos a seguir para su ejecución.

1 INTRODUCCIÓN

La gerencia del E.S.E Hospital de Santa Isabel de Gómez Plata, viene adelantando la implementación de la política de Gobierno Digital, tal como lo establece el decreto 1008 de 2018, cuyas disposiciones se compilan en el Decreto Único Reglamentario del Sector TIC, 1078 de 2015, específicamente en el capítulo 1, titulo 9, parte 2, libro 2; como un instrumento fundamental para mejorar la gestión pública y la relación del Estado con los ciudadanos, la cual, se ha articulado con el Modelo Integrado de Planeación y Gestión como una herramienta dinamizadora para cumplir las metas de las políticas de desarrollo administrativo, articulada a otras políticas esenciales para la gestión pública en Colombia.

Tomando como base el documento técnico de marzo de 2020, el cual nos da a conocer las Políticas de Operación y Proceso de seguridad de la Información. El cual es uno de los insumos principales para la gestión, el control y la toma de decisiones de Función Pública es la información que la entidad genera, almacena y administra, por tanto, es primordial establecer políticas claras y contundentes para la recolección, almacenamiento, administración y entrega de la información.

Por lo anterior, la entidad consolida en el presente documento las políticas en seguridad de la información para garantizar la confidencialidad, integridad, disponibilidad, no repudio y cumplimiento de las obligaciones en materia de tratamiento de datos personales, el buen uso y cuidado de la información y el funcionamiento adecuado de los recursos tecnológicos puestos a disposición de los usuarios.

2 DEFINICIONES

Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.

Amenaza: es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

Causa: Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.

Control o Medida: acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Consecuencia: Resultado de un evento que afecta los objetivos.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.

Estimación del riesgo: Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

Evaluación de riesgos: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

Evento: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

Gestión del Riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.

Identificación del Riesgo: Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

Impacto: son las consecuencias que genera un riesgo una vez se materialice.

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Nivel de Riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.

Proceso: Conjunto de actividades interrelacionadas que apuntan a un objetivo o que interactúan para transformar una entrada en salida.

Probabilidad: es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.

Riesgo: es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.
Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

Seguimiento: Se verifica el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación de los controles de seguridad de la información sobre cada uno de los procesos.

Vulnerabilidad: es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

Valoración del Riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas

3 OBJETIVO

Generar el Plan de Tratamiento de Riesgos de Seguridad de Información como una guía metodológica alineada con el Ministerio de las TIC, que ayudara a gestionar los riesgos que en materia de seguridad y privacidad de la información sea necesario sobre los activos y que sean identificados con una criticidad alta por sus dueños según la valoración dada a su confidencialidad, integridad y su disponibilidad.

3.1 OBJETIVOS ESPECIFICOS

- Mejorar continuamente las capacidades y habilidades necesarias en todos los servidores públicos para identificar, reportar y gestionar los riesgos de seguridad digital mediante acciones de sensibilización y capacitación

- Implementar, mantener y mejorar anualmente el conjunto de controles de seguridad de la información recomendados por el modelo de seguridad y privacidad de la información mediante la aplicación del plan de seguridad y privacidad de la información institucional, para mantener en niveles aceptables los riesgos residuales de seguridad digital.

- Fortalecer continuamente la función institucional mediante la implementación, difusión y mejoramiento continuo del modelo de seguridad y privacidad de la información para mejorar la confianza de las partes interesadas en el compromiso institucional de preservar adecuadamente la confidencialidad, integridad y disponibilidad de la información bajo responsabilidad de la entidad.

4 ALCANCE

El plan de tratamiento de riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación en E.S.E Hospital de Santa Isabel de Gómez Plata, que permita en los procesos de la entidad, integrar las buenas practicas que contribuyan a la toma de decisiones y prevenir incidentes, y de esta forma mejorar los servicios tecnológicos definiendo la pautas para el cumplimiento de los objetivos manejo de la información dentro de la entidad.

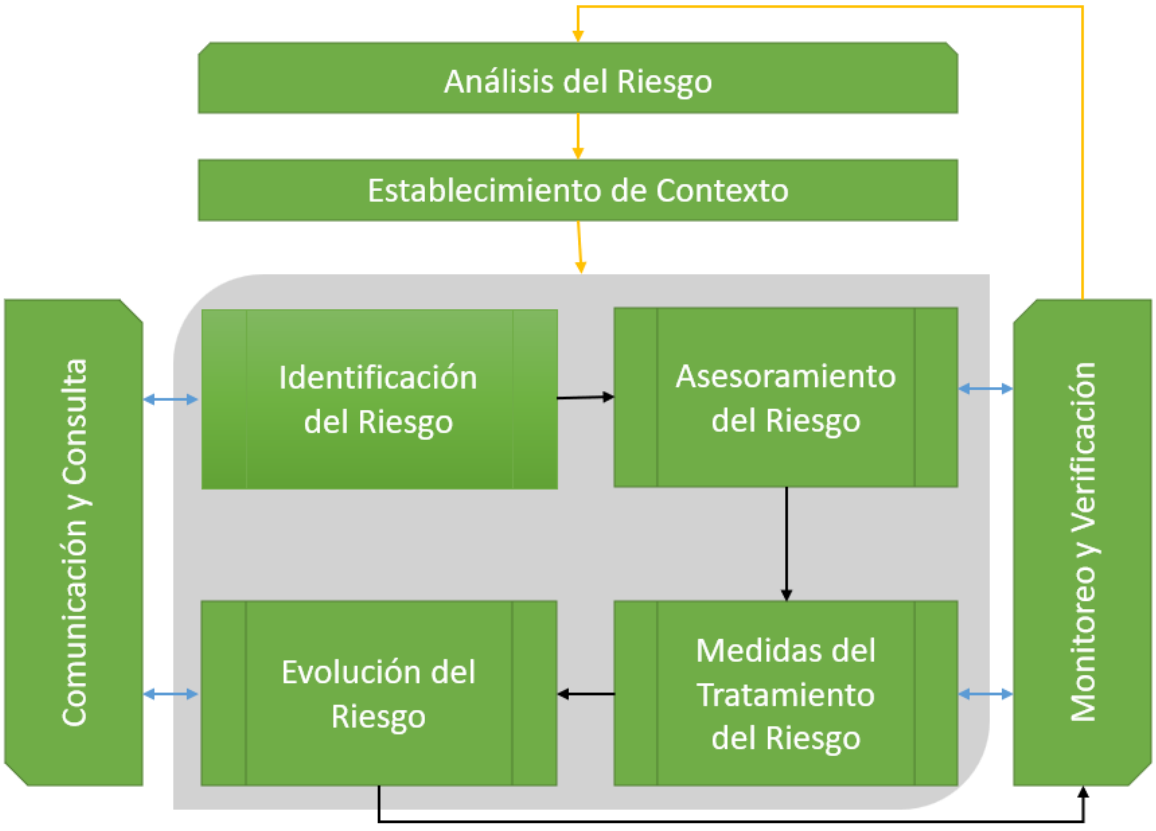
Se tendrá en cuenta los riesgos que se encuentran en los niveles alto y extremo acorde con los lineamientos definidos por el Ministerio de las TIC, con base en las normas vigentes, la metodología definida por la entidad para la gestión del riesgo definida, las pautas y recomendaciones previstas en la ISO 27001 para su seguimiento, monitoreo y evaluación enfocado al cumplimiento y mejoramiento continuo.

4.1 AVANCE DEL TRATAMIENTO DEL RIESGO DE SEGURIDAD Y PRIVACIDAD

El E.S.E Hospital de Santa Isabel de Gómez Plata ha priorizado el proceso de tecnologías de información y de las comunicaciones, en atención al impacto que tiene el mismo sobre los procesos estratégicos, misionales y de apoyo; ya que actualmente, desde el área gerencia todas las actividades de adquisición, implementación y mantenimiento de tecnologías de información y de las comunicaciones para la entidad, por lo cual, una afectación a este proceso, tendrían un impacto alto para el logro de los objetivos hospitalarios.

Sin lugar a dudas, el valor de la seguridad informática de cualquier organización debe redundar en la protección de activos de tecnologías de información, de allí la relevancia de contar con la información que se toma como base para realizar las actividades orientadas a la identificación de riesgos y los planes de tratamiento de datos requeridos para mantener un nivel de riesgo aceptable.

MODELO DE GESTIÓN DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN



6 MARCO REFERENCIAL

6.1 POLÍTICA DE ADMINISTRACION DE RIESGOS

El E.S.E Hospital Santa Isabel de Gómez Plata, a través de su plan de desarrollo, se compromete a dar continuidad con la cultura de gestión del riesgo asociada con la responsabilidad de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector TIC, regulando los riesgos de los procesos y proyectos luchando continuamente contra la corrupción, mediante mecanismos, sistemas y controles enfocados a la prevención y detección de hechos asociados a este fenómeno y fortaleciendo las medidas de control y la eficiencia a lo largo del ciclo de vida del proyecto para optimizar de manera continua y oportuna la respuesta a los riesgos además de los de seguridad y privacidad de la Información y Seguridad Digital de manera Integral.

La política identifica las opciones para tratar y manejar los riesgos basados en la información recolectada del Ministerio TIC en su valoración, que permiten tomar decisiones adecuadas y fijar los lineamientos para administración de los mismos.

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

- **Evitar**: es eliminar la probabilidad de ocurrencia o disminuir totalmente el impacto, lo que requiere la eliminación de la actividad o fuente de riesgo, eliminar la exposición y su expresión máxima es dejar una actividad. Por ejemplo, para evitar perdida de documentación se prohíbe el ingreso a un área.

- **Prevenir**: corresponde al área de planeación, esto es, planear estrategias conducentes a que el evento no ocurra o que disminuya su probabilidad. Un ejemplo de ello son las inspecciones el mantenimiento preventivo, las políticas de seguridad o las revisiones periódicas a los procesos

- **Reducir o mitigar**: corresponde a la protección en el momento en que se presenta el riesgo se encuentra en esta categoría los planes de emergencia planes de continencia equipos de protección personal, ambiental, de acceso mantener copias de respaldo

- **Dispersar**: es dividir una actividad en diferentes componentes operativos, de manera que las actividades no se concentren en un mismo sitio o bajo una sola responsabilidad. Este es el caso de los contratos de suministro de partes, la ubicación de nodos, plantas alternas, equipos paralelos, contratar obras por tramos

- **Compartir**: es involucrar a un tercero para que responda en todo o en parte por el riesgo que genera una actividad. Dentro de los mecanismos de transferencia se encuentran los siguientes: contratos de seguro, transferencia explicita por medio de cláusulas contractuales, derivados financieros.

5 IDENTIFICACIÓN Y CLASIFICACIÓN DE UN RIESGO DE SEGURIDAD

RIESGOS POR GRUPOS DE CATEGORÍAS DE ACTIVOS DE TECNOLOGÍAS INFORMACIÓN			
ESCENARIO DE RIESGO	**GRUPO DE ACTIVO DE TECNOLOGÍA DE INFORMACIÓN**	**AMENAZA**	**VULNERABILIDAD**
Afectación de la disponibilidad, integridad de la información almacenada y confidencialidad de los servidores, por falta en controles sobre la detección contra códigos maliciosos.	SERVIDORES	Operadores de Botnets	Falta en controles de detección contra códigos maliciosos.
Afectación de la disponibilidad, integridad de la información almacenada y confidencialidad de los servidores, por acción de Spyware/Malware, por falta en controles sobre la detección contra códigos maliciosos	SERVIDORES	Spyware/Malware	Falta en controles de detección contra códigos maliciosos.
Afectación de la disponibilidad, integridad de la información almacenada y confidencialidad de los servidores, por acción hackers, debido a una falla en los controles de seguridad informática en la gestión de las redes	SERVIDORES	Hackers	Falta en controles de seguridad informática en la gestión de las redes.

RIESGOS POR GRUPOS DE CATEGORÍAS DE ACTIVOS DE TECNOLOGÍAS INFORMACIÓN			
ESCENARIO DE RIESGO	**GRUPO DE ACTIVO DE TECNOLOGÍA DE INFORMACIÓN**	**AMENAZA**	**VULNERABILIDAD**
Compromiso de la disponibilidad, integridad de los equipos fijos, portátiles, por acción de operadores Botnets, debido a una falta en controles sobre la detección, prevención, recuperación para proteger contra códigos maliciosos	USUARIO	Operadores de Botnets	Falta en controles de detección contra códigos maliciosos.
Compromiso de la disponibilidad, integridad de los equipos fijos, portátiles, por acción de Spyware/Malware, debido a una falta en controles sobre la detección, prevención, recuperación para proteger contra códigos maliciosos.	USUARIO	Spyware/Malware	Falta en controles de detección contra códigos maliciosos.
Compromiso de la disponibilidad, integridad de los equipos fijos, portátiles, por acción de hackers, debido a una falta en controles para los medios removibles.	USUARIO	Hackers	Falta en controles de seguridad informática en la gestión de las redes.

RIESGOS POR GRUPOS DE CATEGORÍAS DE ACTIVOS DE TECNOLOGÍAS INFORMACIÓN			
ESCENARIO DE RIESGO	**GRUPO DE ACTIVO DE TECNOLOGÍA DE INFORMACIÓN**	**AMENAZA**	**VULNERABILIDAD**
Afectación de la disponibilidad, integridad de los sistemas de información web, por acción de hackers, debido a una falta en controles que garanticen el adecuado análisis y especificación de requisitos de seguridad informática en los sistemas de información.	SISTEMAS DE INFORMACIÓN	Hackers	Falta en controles de seguridad informática en la gestión de las redes.
Afectación de la disponibilidad, integridad de los sistemas de información web, por acción de atacantes internos, debido a una falta en controles que garanticen el adecuado análisis y especificación de requisitos de seguridad informática en los sistemas.	SISTEMAS DE INFORMACIÓN	Atacante interno (insider)	Falta en controles que garanticen el adecuado análisis de requisitos de seguridad informática en los sistemas de información
Afectación de la disponibilidad, integridad de los sistemas de información web, por acción de grupos criminales, debido a una falta en controles que garanticen el adecuado análisis de requisitos de seguridad informática en los sistemas.	SISTEMAS DE INFORMACIÓN	Grupos criminales	Falta o deficiencia en controles que garanticen el adecuado análisis y especificación de requisitos de seguridad informática en los sistemas de información

5.1 CLASIFICACIÓN DEL RIESGO

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Tabla 1: Criterios de Clasificación

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Tabla 2: Niveles de Clasificación