Empresa Social del Estado
HOSPITAL MENTAL DE ANTIOQUIA
HOMO

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CONTENIDO

1. OBJETIVO

Detallar el plan de tratamiento de riesgos que hace parte del Sistema de Gestión de Seguridad de la Información – SGSI; de tal forma que se definen y aplican los controles con los cuales se buscan mitigar la materialización de los riesgos de seguridad de la información en la E.S.E Hospital Mental de Antioquia. De esta forma se busca que mediante el tratamiento de los riesgos y la mejora continua de la Seguridad y Privacidad de la Información, las partes interesadas tengan mayor confianza en el tratamiento de la información que se almacena y maneja en la Entidad.

2. ALCANCE

El plan de tratamiento de riesgo tiene alcance para los procesos de la E.S.E Hospital Mental de Antioquia, en concordancia con el alcance del Sistema de Gestion de Seguridad de la Informacion.

3. TERMINOS Y DEFINICIONES

Riesgo: Posibilidad de ocurrencia del evento que tiene un efecto positivo o negativo sobre el producto o servicio generado de un proceso o el cumplimiento de los objetivos institucionales.

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información. Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta en el beneficio que se genera.

También se pueden generar riesgo positivo en la seguridad de la información por el aprovechamiento de oportunidades y fortalezas que se presenten.

Riesgo positivo: Posibilidad de ocurrencia de un evento o situación que permita optimizar los procesos y/o la gestión institucional, a causa de oportunidades y/o fortalezas que se presentan en beneficio de la entidad.

Seguridad de la información: Este principio busca crear condiciones de uso confiables en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.

4. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

En el marco del Modelo de Seguridad y Privacidad de la Información y el Sistema de Gestion de Seguridad de la Información –SGSI de la E.S.E Hospital Mental de Antioquia, se busca prevenir los efectos no deseados que se puedan presentar en cuanto a seguridad de la información, por lo cual es importante controlar y establecer los riesgos de seguridad de la información.

De esta forma, se garantiza el tratamiento de los riesgos de seguridad de la información y la gestión de riesgo positivo u oportunidad, acorde con lo establecido en el **MATRIZ GESTION DEL RIESGO GC-FR-12.**

5. RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

A continuación se visualizan los riesgos de Seguridad de la Información, los cuales se encuentran asociados al Sistema de Gestion de Seguridad de la Información- SGSI de la E.S.E Hospital Mental de Antioquia.

PROCESO:	SISTEMAS DE INFORMACION
OBJETIVO	Establecer procedimientos para la planeación, registro, almacenamiento, tratamiento, comunicación y presentación de información institucional, que garantice datos oportunos y confiables para la toma de decisiones.
FECHA:	14 de agosto 2019
RESPONSABLE:	Lider Proceso Sistemas de Informacion

IDENTIFICACION DEL RIESGO					ANALISIS DEL RIESGO								VALORACION DEL RIESGO							
					CALIFICACION								Análisis y evaluación de los controles para mitigar				NUEVA CALIFICACION			
					EVALUACION INHERENTE DEL RIESGO															
CONSECUTIVO	RIESGO (FALLO O EVENTO)	DESCRIPCION	CAUSAS	CONSECUENCIAS	PROBABILIDAD	IMPACTO	IMPACTO RIESGO DE CORRUPCION	TIPO DE IMPACTO	EVALUACIÓN INHERENTE DEL RIESGO	MEDIDAS DE RESPUESTA	CONTROLES	TIPO DE CONTROL	Evaluación del diseño del control	Evaluación de la ejecución del control	Solidez de cada control	Solidez del conjunto de controles	PROBABILIDAD	IMPACTO	IMPACTO RIESGO DE CORRUPCION	EVALUACIÓN RESIDUAL DEL RIESGO
R 1	OPERATIVO TECNOLOGICO (Fallas eléctricas)	Sobrecarga del sistema al conectar mas equipos de los que permite la capacidad instalada de la corriente de distribución.	Cableado eléctrico sobrecargado de equipos conectados.	a) Daño en equipos b) Pérdida de información c) Incendio.	3	2		Operativo perdida de información	Moderada	Evitar el riesgo	Diseño y planeación de la distribución de los puntos de conexión eléctricos de cada una de las dependencias de la institución	Preventivo	100	Fuerte	Fuerte	FUERTE	1	1		Baja
R 2	OPERATIVO TECNOLOGICO CUMPLIMIENTO (Desactualización de tecnología computacional)	Obsolescencia de las herramientas informáticas de la institucional que no permite obtener una información rápida, confiable, confidencial y disponible y con mayor facilidad para su interpretación, afectación en la seguridad informática de la entidad ya el spyware o programa informático no actualiza los controles mínimos que se deben de tener dentro la plataforma tecnológica corporativa, solo de esta forma se podrá garantizar la custodia, privacidad y confidencialidad de la información.	Desactualización de las herramientas informáticas.	a) Falta de credibilidad en la obtención de los datos b) Carencia de datos confiables para la toma de decisiones en la institución C) Exposición y compromiso de la seguridad informática del a institución	3	2		Imagen Operativo Financiero	Moderada	Evitar el riesgo	Ejecución del plan de renovación y tecnológica	Preventivo	100	Fuerte	Fuerte	FUERTE	1	1		Baja
R 3	OPERATIVO TECNOLOGICO CUMPLIMIENTO (Desconocimiento del estado lógico y físico de la plataforma informática)	Incumplimiento al monitoreo del estado en el que se encuentra la plataforma informática y los equipos de la institución	a) Inexistencia de software de verificación del inventario de red	a) Pérdida de información b) Falta de información veridica y en tiempo real del estado de los equipos y a red c) Ausencia de red por falta de gestión y control de la misma d) exposición de la seguridad y privacidad de la información	3	2		Imagen Operativo Financiero	Moderada	Evitar el riesgo	La adquisición de software por parte del institución	Preventivo	100	Fuerte	Fuerte	FUERTE	1	1		Baja
			b) La intervención de los usuarios al instalar software sin autorización o ilegal								Configuración de directiva de los equipos por parte de la oficina de sistemas que restringa la instalación de cualquier software	Preventivo	100	Fuerte	Fuerte					
			c) Interrupción o latencia de la red de datos en relaciones de trabajo								Mantenimientos preventivos a los dispositivos activos de la red y a la infraestructura tecnológica completa y la completa actualización de los registros de activos fijo de la institucion	Preventivo	100	Fuerte	Fuerte					
R 4	OPERATIVO Daño o hurto en la red o en los servidores de la Entidad por ingreso de personal ajeno al área	Ingreso de personas ajenas a la oficina de sistemas que puedan causar un daño en la red o en los servidores de la Entidad o hurto de equipos	a) No se cuenta con un control de ingreso de personas ajenas a la oficina de sistemas b)No existe una de políticas de accesos no autorizados y restringidos a personal externo al area de sistemas	a) Pérdida de elementos del área B) Hérdida o daños en la información c) Fuga de información confidencial	4	5		Operativo perdida de información	Extrema	Reducir el riesgo	Establecer un lineamiento de restricciones de acceso físico a la oficina de sistemas por tarta del personal	Preventivo	100	Fuerte	Fuerte	FUERTE	2	3		Alta
R 5	TECNOLOGICO OPERATIVO Perdida de información por virus, malware y ransomware	La incapacidad de acceder a cualquier dato desde un sistema de computación en funcionamiento o una copia de seguridad, por ataques de virus, malware y ransomware	Antivirus desactualizado que no detecta los virus mas recientes	a) Hérdida de información b) Daño irrecuperable de la información en la entidad	3	4		Operativo	Extrema	Reducir el riesgo	Disponer de una site de herramientas actualizadas que permitan el control desde y hacia internet y los dispositivos externos , memorias USB y discos portátiles	Preventivo	100	Fuerte	Fuerte		1	2		Baja
R8	ESTRATEGICO OPERATIVO	La posibilidad que un agente ajeno a la entidad viole el acceso a la información estratégica de la institución	perdida de la confidencialidad de la información	a)Perdida de la información b) Daño irrecuperable de la información en la entidad Fuga de información confidencial	2	5			Extrema	Evitar el riesgo	Establecer permisos de acceso, visualización y escritura para los diferentes recursos informáticos de la entidad y que los permisos sean acordes a puesto del funcionario	Preventivo	100	Fuerte	Fuerte	FUERTE	1	3		Moderada
			Integridad o modificación no autorizadas de la información								Verificar los usuarios en el sistema de información y habilitación de la auditorias de los registro		100	Fuerte	Fuerte					
			Perdida de la disponibilidad de la información								Backupde seguridad veces al dia		100	Fuerte	Fuerte					

6. ACTIVIDADES A DESARROLLAR SOBRE LOS RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Para el manejo de los riesgos se deben analizar las posibles acciones a emprender, las cuales deben ser factibles y efectivas, tales como: la implementación de las políticas, definición de estándares, optimización de procesos y procedimientos y cambios físicos entre otros. El tratamiento de riesgos implica tomar decisiones basadas en los resultados de la identificación de riesgos y su análisis.

La política de gestión de riesgos está determinada por las siguientes opciones de tratamiento:

La política de gestión de riesgos está determinada por las siguientes opciones de tratamiento:

Zonas o niveles de criticidad e intervención del riesgo		Tratamiento
Zona de Riesgo Bajo	Dada su baja probabilidad de presentación, es posible asumir el riesgo, pero deben planearse acciones para reducirlo en caso que se presente.	Asumir el riesgo
Zona de Riesgo Moderada	Evaluada la probabilidad e impacto es posible asumir el riesgo, pero siempre acompañado de acciones para reducirlo y evitarlo en lo posible.	Asumir el riesgo, Reducir el riesgo
Zona de Riesgo Alta	En esta zona de riesgo alta debe siempre evitar, reducir, compartir o transferir el riesgo.	Reducir el riesgo, evitar, compartir o transferir
Zona de Riesgo Extrema	En esta zona de riesgo extrema debe siempre y de manera simultánea: evitarse el riesgo, reducirlo y compartir o transferir el riesgo. Los puntos de control deben ser más estrictos	Reducir el riesgo, evitar, compartir o transferir

La política de gestión del riesgo está alineada con el modelo institucional y es una de las fuentes de mejora, Para el tratamiento, especialmente en los casos que se identifican nuevos riesgos, cuando es necesario rediseñar los controles existentes o definir unos nuevos controles.

7. MECANISMOS DE SEGUIMIENTO Y VERIFICACIÓN

Los atributos establecidos para valorar el desempeño de la gestión de riesgos es una parte de la evaluación global de la institución y de la medición del desempeño de las áreas y de las personas.

Las valoraciones integrales de toda la institución y particulares por proceso, proyecto o estrategia correspondiente a la disminución del nivel de vulnerabilidad, por lo que se tiene el siguiente indicador.

8. MARCO LEGAL

- Constitución Política de Colombia 1991, articulo 15, reconoce como derecho fundamental el Habeas Data y articulo 20, Libertad de información.
- Decreto 612 de 4 de abril de 2018, por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al plan de acción por parte de las Entidades del Estado.
- Decreto 1008 de 14 de junio de 2018, por el cual se establecen los lineamientos generales de la política de Gobierno digital.
- Guía 7 gestión de riesgos. Modelo de Seguridad y Privacidad de la Información. Ministerio de las Tecnologías y la información y las comunicaciones, estrategia de Gobierno Digital.
- Guía 8 controles de seguridad y privacidad de la información. Modelo de seguridad y privacidad de la información. Ministerio de las Tecnologías y la información y las comunicaciones, estrategia de Gobierno Digital.

9. DOCUMENTOS ASOCIADOS

- **MATRIZ GESTION DEL RIESGO GC-FR-12.**
- **MANUAL DE SISTEMAS DE INFORMACIÓN SI-MA - 01**

10. RESPONSABLE DEL DOCUMENTO

Profesional Universitario de Sistemas