

E.S.E. HOSPITAL NUESTRA SEÑORA DEL CARMEN DE TABIO

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

[Escriba el subtítulo del documento]

Tabla de contenido

1. **INTRODUCCION** 3
2. **OBJETIVOS:** 3
3. **ALCANCE** 3
4. **RESPONSABLES** 3
5. **DESCRIPCION DEL PLAN** 4
6. **RECURSOS:** 5
7. **PLAN DE ACTIVIDADES – CRONOGRAMA** 6
8. **INDICADORES** 6
9. **ANEXOS:** 6
10. **BIBLIOGRAFÍA:** 6
11. **CONTROL DE CAMBIOS:** 6
12. **REVISIÓN Y APROBACIÓN:** 7

1. INTRODUCCION

El plan de tratamiento de seguridad de la información tiene como propósito de definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad Digital que el Hospital Nuestra Señora Del Carmen De Tabio pueda estar expuesto, y de esta manera alcanzar el plan estratégico, los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad y disponibilidad de la información.

2. OBJETIVOS:

La gestión de riesgos constituye una estrategia con el los principales Objetivos de esta gestión son:
Gestionar riesgos de Seguridad y Privacidad de la información, Seguridad Digital, de acuerdo con los contextos establecidos en la Entidad.
Fortalecer y apropiar conocimiento referente a la gestión de riesgos Seguridad y Privacidad de la información, Seguridad Digital.
Emplear un enfoque de sistemas para planificar, implementar, monitorizar y gestionar los riesgos de seguridad digital.

3. ALCANCE

Con el propósito de realizar una eficiente gestión de riesgos de Seguridad Digital en el Hospital Nuestra Señora Del Carmen De Tabio, esta actividad se debe realizar integrando los procesos de la entidad con este plan, mediante el uso de buenas prácticas y lineamientos, con el propósito que ello contribuya a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos.

A partir de lo anterior se definen los lineamientos mediante una guía de para la gestión de riesgos de Seguridad Digital, para el tratamiento de los riesgos asociados a la información que es soportada por compontes tecnológicos en el entorno digital.

Tener como punto a favor copias de seguridad de bases de datos y la información interna, para así mitigar robo de información

4. RESPONSABLES

Oficina de Sistemas y Comunicaciones

5. DESCRIPCION DEL PLAN

El Hospital Nuestra Señora Del Carmen De Tabio través de su Modelo de Seguridad y Privacidad, se compromete a mantener una cultura de la gestión del riesgo digital, con un enfoque basado en los riesgos de seguridad digital en los procesos y proyectos luchando continuamente contra la corrupción, mediante mecanismos, sistemas y controles enfocadosa 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 su valoración, permiten tomar decisiones adecuadas y fijar los lineamientos para administración de los mismos; a su vez, transmiten la posición de la dirección y establecen las guías de acción necesarias a todos los colaboradores del Hospital.

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 del activo, eliminarla exposición y su expresión máxima es dejar una actividad. Por ejemplo, para evitarperdida de archivos se retiran los permisos de acceso.

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

Controlar: Corresponde a la administración del sistema hospitalario, quien maneje el mismo, debe estar capacitado para su uso, debe manejarse sobre el código de ética.

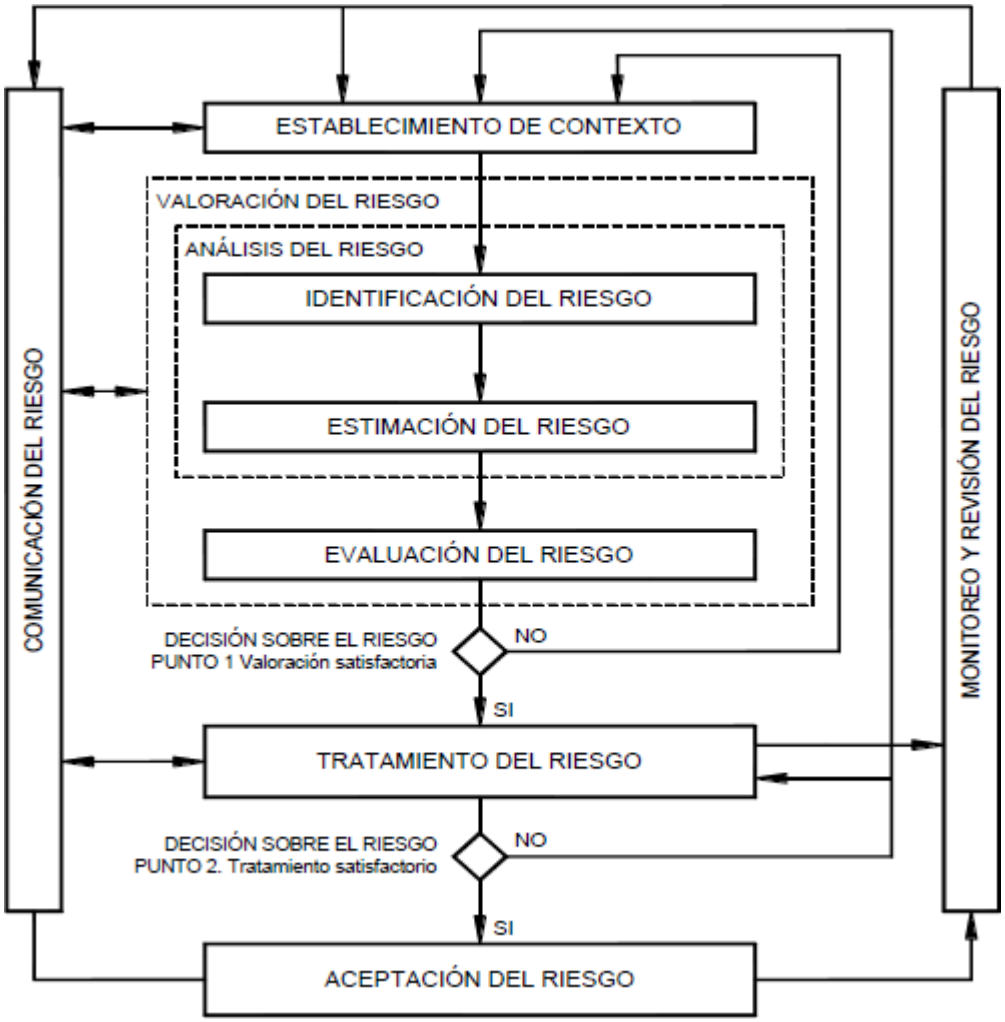


DIAGRAMA DE FLUJO : En la figura siguiente se presenta el modelo de gestión de riesgos de seguridad de la información basado tanto en la norma ISO/IEC 31000 como en la ISO 27005 para la adecuada administración de riesgos en la seguridad de la información; los elementos que lo componen.

6. RECURSOS:

RECURSOS	VARIABLE
Colaboradores	La Oficina de Tecnologías de la información a través de seguridad de la información es responsable de coordinar, implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos en la Entidad en lo concerniente a la seguridad y privacidad de la información lo cual contribuyea la mejora continua.

7. PLAN DE ACTIVIDADES – CRONOGRAMA

				VIGENCIA 202															
ÍTEM		ACTIVIDADES		ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEPT	OCT	NOV	DIC	TOTAL EJECUTADO	TOTAL PROGRAMADO	PENDIENTE POR EJECUTAR	PORCENTAJE DE EJECUCIÓN	RESPONSABLE	OBSERVACIONES
1		MANTENER EL HOSPITAL CON ANTIVIRUS LICENCIADO	E P %													0	1	1	0%	Personal de sistemas	
		MANTENER EL FIREWARE ACTIVO (SVRHNSCTABIO)	E P %													0	2	2	0%	Personal de Sistemas	
2		POR MEDIO DE CORREO ELECTRONICO SE SOCIALIZA EL USO ADECUADO DE LOS CELULARES CORPORATIVOS	E P %													0	2	2	0%	Personal de Sistemas	
		MANTENER EL ARBOL MAGNETICO LIBRE DE ATAQUES EXTERNOS CON EL FIREWARE ACTIVO	E P %													0	2	2	0%	Personal de Sistemas	
3		TENER PUBLICADA LA POLITICA DE TRATAMIENTO DE DATOS EN LA PAGINA WEB	E P %													0	2	2	0%	Personal de Sistemas	

8. INDICADORES

MANTENER LOS EQUIPOS DE COMPUTO DEL HOSPITAL CON ANTIVIRUS	**N° DE EQUIPOS CON ANTIVIRUS VIGENTE**	**N° TOTAL DE EQUIPOS DE LA INSTITUCIÓN EN USO.**
	100	**100**

9. ANEXOS:

POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

10. BIBLIOGRAFÍA:

https://www.pmg-ssi.com/2014/01/isoiec-27005-gestion-de-riesgos-de-la-seguridad-la-informacion/

https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

11. CONTROL DE CAMBIOS:

Tabla. Control de Cambios en este Documento

FECHA	VERSIÓN	No. SOLICITUD DE ACTUALIZACIÓN	CAMBIO REALIZADO	RESPONSABLE
2021-01-15	01	Creación	Creación	Líder de Sistemas
2022-01-14	02	Actualización	Actualización y ajuste de contenido	Líder de Sistemas
2023-01-20	03	Actualización	Actualización y ajuste de contenido	Líder de Sistemas
2024-01-22	04	Actualización	Actualización y ajuste de contenido	Líder de Sistemas

12. REVISIÓN Y APROBACIÓN:

Nombre	Fabián Pulido	Jenny Pilar Gómez Plazas	Isabel Rocio Garzón Forero
Cargo	Líder de Sistemas	Asesora de Planeación	Gerente
	Elaboró	Revisó	Aprobó