	HOSPITAL REGIONAL DE SOGAMOSO E.S.E.	CÓDIGO:
	PLAN ANTICORRUPCIÓN Y ATENCIÓN AL CIUDADANO	VERSIÓN:
	PLAN	FECHA:
		PÁGINA 1 de 9

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

2022

CONTROL DE CAMBIOS

No. VERSIÓN	DESCRIPCIÓN DEL CAMBIO	FECHA
01	Elaboración y emisión plan de tratamiento de riesgos de seguridad y privacidad de la información	

	ELABORÓ	REVISÓ	APROBÓ
FECHA			
FIRMAS			
NOMBRE	YEILER EDUARDO BERNAL	OSCAR DARÍO SOLER M.	DIEGO FERNANDO FUQUEN F.
CARGO	Lider Oficina de Sistemas	Asesor de Planeación	Subgerente Administrativo y Financiero

Tabla de contenido

INTRODUCCION	3
OBJETIVOS	4
Objetivo general	4
Objetivos específicos	4
ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	5
PROCESO PARA EL TRATAMIENTO DE RIESGOS DE SEGURIDAD PRIVACIDAD DE LA INFORMACIÓN.....	5
CRONOGRAMA PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION.....	7
Planeación Gestión del riesgo:	7
Identificación de activos:	7
Amenazas y vulnerabilidades:	8
Determinación del riesgo	8
Análisis de Riesgo:.....	8
Gestión del riesgo:	8
Planificación de controles:	8
Monitoreo y seguimiento:.....	8
VENTAJAS DE ESTABLECER UN PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	9

INTRODUCCION

El Hospital Regional de Sogamoso E.S.E., Realiza la formulación y construcción del Plan de tratamiento de riesgos de seguridad y privacidad de la información y de cada uno de los componentes que hacen parte de este.

Reconociendo la información como un activo primordial para la organización, y su entorno, se debe garantizar la protección y confidencialidad de esta en todos los niveles de la estructura organizacional

El hospital regional de Sogamoso E.S. E y cada una de sus unidades básicas de atención, garantizan el estricto cumplimiento de los principios de confidencialidad, integridad y disponibilidad. Esto con el fin de generar confianza dentro y fuera de la organización en el uso adecuado y pertinente de la información.

Debido al alto flujo de información, producto de la actividad de la entidad, es necesario crear una cultura preventiva organizacional enfocada en la correcta administración y custodia de la información.

OBJETIVOS

Objetivo general

Estructurar e implementar el 100% del plan de tratamiento de riesgos de seguridad y privacidad de la información, de acuerdo con los lineamientos y normativa vigente, con el fin de adoptar medidas y políticas que garanticen el adecuado tratamiento de los riesgos a los que se enfrenta la información y su consecuencia dentro de la organización.

Objetivos específicos

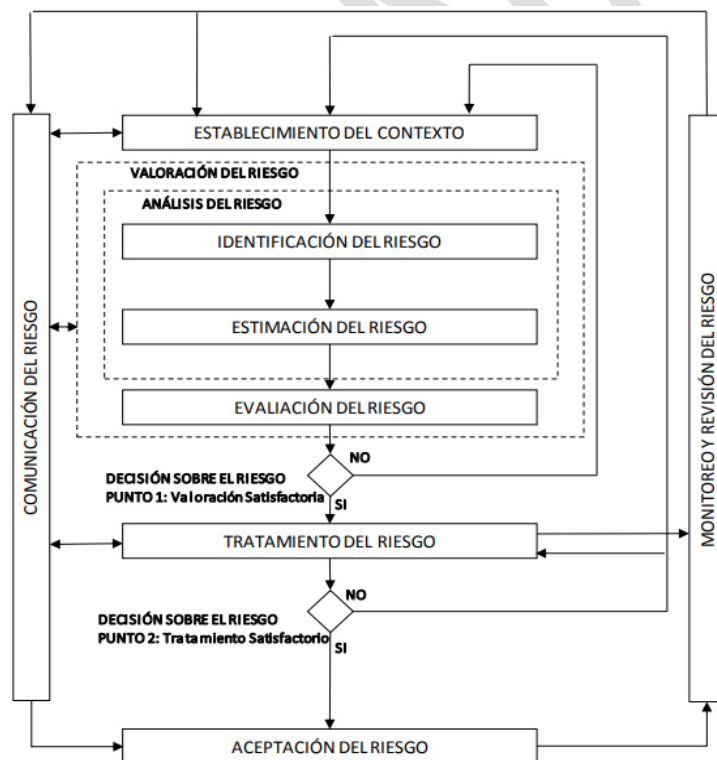
- Estructurar y consolidar un plan de tratamiento de riesgos de seguridad y privacidad de la información, pertinente y oportuno para el hospital regional de Sogamoso E.S.E
- Generar estrategias que permitan afianzar dentro del personal del hospital, una cultura enfocada en la protección de la información y la mitigación del riesgo de seguridad en la información
- Aplicar el plan de tratamiento de riesgos de seguridad y privacidad de la información a cada uno de los activos de información de la entidad y sus dependencias.
- Desarrollar o actualizar el inventario de activos de la información

ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Para el Hospital Regional Sogamoso E.S.E la estructuración y puesta en marcha de un Plan de seguridad de la información, tiene un carácter vinculante para cada una de las dependencias y recurso humano que hacen parte de la entidad, de tal manera que genere sinergia dentro de la organización, y bajo parámetros y principios básicos se gestione el activo de la información, garantizando los principios de confidencialidad, integridad y disponibilidad.

Los lineamientos establecidos en el plan, deberán ser socializados y apropiados por todos los funcionarios, contratistas etc., por su carácter vinculante y aplicable a procesos estratégicos, misionales o de apoyo para el Hospital.

PROCESO PARA EL TRATAMIENTO DE RIESGOS DE SEGURIDAD PRIVACIDAD DE LA INFORMACIÓN



Fuente: https://www.mintic.gov.co/gestioni/615/articles-5482_G7_Gestion_Riesgos.pdf

Para la evaluación del riesgo de seguridad y privacidad de la información, se tomará como referencia la matriz de activos de la información, que se describe como un insumo fundamental para realizar gestión de riesgos a los activos de información que se consideren con nivel de clasificación ALTA dependiendo de los criterios de

clasificación: Confidencialidad, Integridad y Disponibilidad tengan la siguiente calificación

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

Fuente: https://www.mintic.gov.co/gestioni/615/articles-5482_G7_Gestion_Riesgos.pdf

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.

Fuente: https://www.mintic.gov.co/gestioni/615/articles-5482_G7_Gestion_Riesgos.pdf

CRONOGRAMA PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Fase	Actividad	Responsable	F/ inicio	F/terminaci3n
Planeaci3n gesti3n del riesgo	Revisar y ajustar metodolog3a para la gesti3n de Riesgo			
Identificaci3n de activos	identificaci3n ,clasificaci3n y valoraci3n de activos de la informaci3n			
Amenazas y vulnerabilidades	identificaci3n de amenazas y vulnerabilidades			
Determinaci3n de riesgos	Determinar impacto amenaza por activo			
An3lisis de riesgos	Calculo de riesgos			
Gesti3n de riesgos	Determinaci3n , dise1o y priorizaci3n de controles			
Planificaci3n de controles	Implementaci3n de controles (sin recursos) planificaci3n controles (recursos)			
Monitoreo y seguimiento	Medici3n de la eficacia de los controles			

Planeaci3n Gesti3n del riesgo: Definici3n de metodolog3a y estrategias aplicar para realizar la correcta estructuraci3n de la planeaci3n del riesgo en la entidad, Esta etapa es orientadora, se centra en determinar las amenazas y debilidades de la entidad, de su correcto an3lisis, se pueden inferir las causas del riesgo.

Identificaci3n de activos: esta etapa est3 dirigida a identificar, clasificar y valorar todos los activos de informaci3n de la organizaci3n. d3nde est3n?, 1tipo de informaci3n? estado, responsables, medios f3sicos, magn3ticos en la nube, etc.

Los activos de la informaci3n se pueden clasificar en primarios y de soporte, para los primeros se identifican los siguientes:

Procesos: Cuya perdida imposibilita el cumplimiento de la misi3n institucional, procesos claves para el logro de requisitos legales o contractuales.

Informaci3n: Activo vital para la ejecuci3n de la actividad, puede involucrar caracter3sticas de tipo confidencial, estrat3gica o de alto costo para la organizaci3n

Actividades y procesos: Si se degradan o adquieren vicios, imposibilitan el cumplimiento de los objetivos

Para la clasificaci3n de soporte se tiene:

Hardware: Elementos f3sicos que dan soporte a los procesos

Software: Todas aquellas herramientas, programas, aplicaciones que dan soporte a procesos dentro de una entidad.

Redes: Dispositivos de las telecomunicaciones que permiten interconectar dispositivos electr3nicos.

Personal: Gesti3n humana involucrada en los sistemas de informaci3n

Amenazas y vulnerabilidades: Es la etapa que permite conocer los eventos potenciales, internos o externos que ponen en riesgo el logro de la misión, estableciendo las causas y consecuencias de la ocurrencia del riesgo.

Determinación del riesgo: La determinación del riesgo busca establecer la probabilidad de ocurrencia del mismo y sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo. En este punto es importante destacar que se pueden tener en cuenta algunos criterios para evaluar el riesgo de seguridad.

- Criticidad de los activos
- Requisitos legales y reglamentarios
- Disponibilidad, integridad y confidencialidad
- El buen nombre de la institución

Análisis de Riesgo: Etapa orientada al cálculo de la materialización del riesgo, Se han establecido dos aspectos a tener en cuenta en el análisis de los riesgos identificados:

Probabilidad: la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de Frecuencia, si se ha materializado, o de Factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado.

Impacto: Consecuencias que puede ocasionar la materialización del riesgo.

Gestión del riesgo: Es la etapa de la determinación de los controles, el tratamiento de los riesgos, diseño y priorización de controles estructurados para la entidad.

Planificación de controles: Fase de implementación de controles desarrollados para la organización

Monitoreo y seguimiento: En esta etapa se puede identificar en qué medida los controles identificados están aportando para disminuir los niveles de probabilidad e impacto del riesgo. Verificando pertinencia y efectividad.

Los riesgos son dinámicos y se pueden transformar, por tal motivo es necesario realizar un continuo seguimiento que detecte cambios aumentos o nuevas amenazas que pueda surgir.

VENTAJAS DE ESTABLECER UN PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

- Clasificación y organización de los activos de información
- Identificación de posibles riesgos en los activos de la información
- Generación de líneas de defensa para la información
- Identificación de soportes de respaldo para los activos de la información
- Definición de responsables para los activos de la información
- Generación de cultura organizacional dirigida a la confidencialidad, integridad y disponibilidad de la información.
- Disminución de pérdida de información
- Disminución de costos operativos
- Credibilidad de la institución

