PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD YPRIVACIDAD DE LA INFORMACION

2024

No. VERSIÓN	DESCRIPCIÓN DEL CAMBIO	FECHA
01	Elaboración y emisión plan de tratamiento de riesgos de seguridad y privacidad de la información	15/02/2022
02	Actualización Vigencia 2024	30/01/2024

	ELABORÓ	REVISÓ	APROBÓ
FECHA	30/01/2024	30/01/2024	30/01/2024
FIRMAS	FIRMADO EN ORIGINAL	FIRMADO EN ORIGINAL	FIRMADO EN ORIGINAL
NOMBRE	YEILER EDUARDO BERNAL GUTIERREZ	OSCAR DARIO SOLER MORALES	DIEGO FERNANDO FUQUEN F.
CARGO	Líder de Gestión de la Tecnología	Asesor de planeación	Subgerente Administrativo y Financiero

Tabla de contenido

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

MARCO NORMATIVO

NORMA	DESCRIPCION
Decreto 1078 de 2015	**Por medio del cual se expide el decreto único reglamentario del sector de tecnologías de la información y las comunicaciones**
DECREETO 1008 DE 2018	**Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.**
CONPES 3854 de 2016	**Política Nacional de Seguridad Digital**
Manual para la Implementación de la Política de Gobierno Digital	**Implementación de la política de Gobierno Digital. Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2) Versión 7, abril de 2019**
Modelo de Seguridad y privacidad de la información - MSPI	**Se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Política de Gobierno Digital, TIC para el Estado y TIC para la Sociedad. TIC, que son habilitados por tres elementos transversales: Seguridad de la Información,**

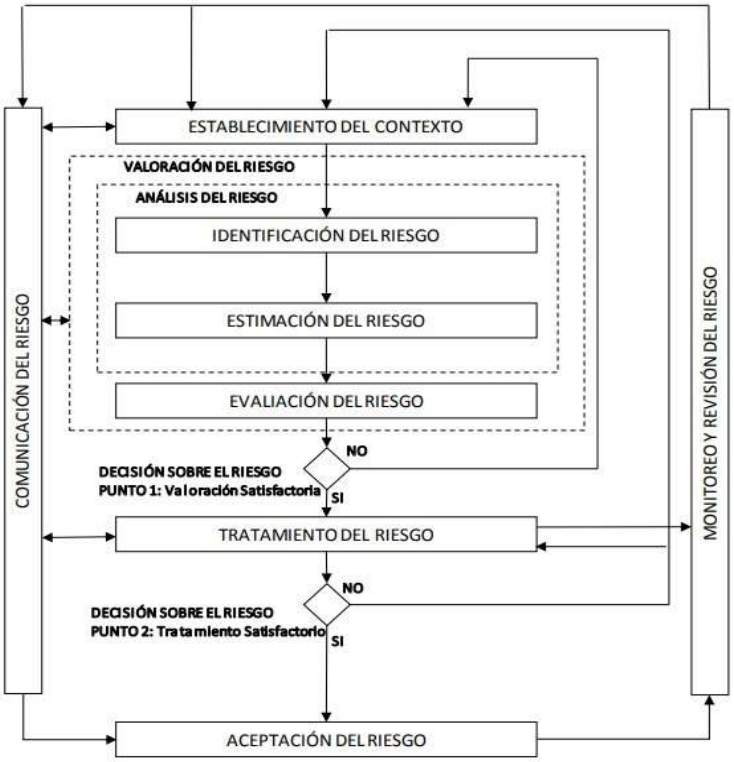
	Arquitectura y Servicios Ciudadanos Digitales
NTC / ISO 27001:2013	**Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).**
NTC/ISO 31000:2009	**Gestión del Riesgo. Principios y directrices.**
Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 4	**Riesgos de Gestión, Corrupción y Seguridad Digital Función Pública octubre 2018**

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/gestionti/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 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

Fuente: https://www.mintic.gov.co/gestionti/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/gestionti/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/terminació
Planeación gestión del riesgo	Revisar y ajustar metodología para la gestión de Riesgo			
Identificación de activos	identificación, clasificación y valoración de activos de la información			
Amenazas y vulnerabilidades	identificación de amenazas y vulnerabilidades			
Determinación de riesgos	Determinar impacto amenaza por activo			
Análisis de riesgos	Cálculo de riesgos			
Gestión de riesgos	Determinación, diseño y priorización de controles			
Planificación de controles	Implementación de controles (sin recursos) planificación controles (recursos)			
Monitoreo y seguimiento	Medición de la eficacia de los controles			

Planeación Gestión del riesgo: Definición de metodología y estrategias aplicar para realizar la correcta estructuración de la planeación del riesgo en la entidad, Esta etapa es orientadora, se centra en determinar las amenazas y debilidades de la entidad, de su correcto análisis, se pueden inferir las causas del riesgo.

Identificación de activos: esta etapa está dirigida a identificar, clasificar y valorar todos los activos de información de la organización. dónde están?, ¿tipo de información? estado, responsables, medios físicos, magnéticos en la nube, etc.

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

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

Información: Activo vital para la ejecución de la actividad, puede involucrar características de tipo confidencial, estratégica o de alto costo para la organización

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

Para la clasificación de soporte se tiene:

Hardware: Elementos físicos 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 electrónicos.

Personal: Gestión humana involucrada en los sistemas de información

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 perdida de información
- Disminución de costos operativos
- Credibilidad de la institución

	HOSPITAL REGIONAL DE SOGAMOSO E.S.E		**CÓDIGO:** D-PI-FT-001
	PLAN OPERATIVO ANUAL		**VERSIÓN:** 02
			FECHA: 30/12/2020
	FORMATO		**PÁGINA:**

Nombre del Proceso: Gestión de Recursos Informáticos

Objetivo del Proceso: Planificar el desarrollo institucional del Hospital Regional de Sogamoso E.S.E. en el corto, mediano y largo plazo, mediante la formulación, ejecución, seguimiento, monitoreo y evaluación de planes, programas y proyectos, con el fin de garantizar el cumplimiento de objetivos y metas establecidas.

Líder del Proceso: YEILER EDUARDO BERNAL GUTIERREZ | **Fecha de Elaboración:** | **30/01/2024**

ÍTEM	OBJETIVO	META	ACTIVIDAD	INDICADOR	EJECUCIÓN																																																RESPONSABLE DE LA ACTIVIDAD	EVIDENCIA DE LA ACTIVIDAD	INCLUIDO EN EL PAA		PRESUPUESTO
					ENERO				FEBRERO				MARZO				ABRIL				MAYO				JUNIO				JULIO				AGOSTO				SEPTIEMBRE				OCTUBRE				NOVIEMBRE				DICIEMBRE						SI	NO	
					sem 1	sem 2	sem 3	sem 4	sem 1	sem 2	sem 3	sem 4	sem 1	sem 2	sem 3	sem 4	sem 1	sem 2	sem 3	sem 4	sem 1	sem 2	sem 3	sem 4	sem 1	sem 2	sem 3	sem 4	sem 1	sem 2	sem 3	sem 4	sem 1	sem 2	sem 3	sem 4	sem 1	sem 2	sem 3	sem 4	sem 1	sem 2	sem 3	sem 4	sem 1	sem 2	sem 3	sem 4	sem 1	sem 2	sem 3	sem 4					
1	Diseñar Estrategias que permitan mitigar la materialización de los riesgos de seguridad y privacidad de la información	Cumplir con el 100 % de las actividades planteadas en el plan de tratamiento de riesgos de la información	Revisión del plan de tratamiento de riesgos de la seguridad y privacidad de la información por parte del comité institucional de gestión y desempeño	Plan de tratamiento de riesgos de la seguridad y privacidad de la información revisado por parte del comité institucional de gestión y desempeño																																															**Comité institucional de gestión y desempeño**	Acta comité institucional de gestión y desempeño interno lista de asistencia			
		Realizar la revisión y actualización del 100% del mapa de riesgo de seguridad y privacidad de la información	Actualización del mapa de riesgos de seguridad y privacidad de la información	(Numero de procesos con mapa de riesgos en áreas de la entidad de la entidad / N° áreas de la entidad) * 100																																															**Líder de planeación líder de sistemas**	mapa de riesgos de la información actualizado de cada proceso			
		Socializar el 100% de los riesgos de Seguridad y privacidad de la información identificados en la entidad	Realizar 3 Socializaciones del mapa de riesgos de Seguridad y privacidad de la información en las diferentes áreas de la entidad	N° de socializaciones del mapa de riegos en áreas de la entidad /N° áreas de la entidad *100																																															**Líder de planeación líder de sistemas**	Correo electrónico a lideres de proceso			

	HOSPITAL REGIONAL DE SOGAMOSO E.S.E	**CÓDIGO:** D-PI-FT-001
	PLAN OPERATIVO ANUAL	**VERSIÓN:** 02
		FECHA: 30/12/2020
	FORMATO	**PÁGINA:**

Nombre del Proceso: Gestión de Recursos Informáticos

Objetivo del Proceso: Planificar el desarrollo institucional del Hospital Regional de Sogamoso E.S.E. en el corto, mediano y largo plazo, mediante la formulación, ejecución, seguimiento, monitoreo y evaluación de planes, programas y proyectos, con el fin de garantizar el cumplimiento de objetivos y metas establecidas.

Líder del Proceso: YEILER EDUARDO BERNAL GUTIERREZ	**Fecha de Elaboración:**	**30/01/2024**

ÌTEM	OBJETIVO	META	ACTIVIDAD	INDICADOR	EJECUCIÓN																																																RESPONSABLE DE LA ACTIVIDAD	EVIDENCIA DE LA ACTIVIDAD	INCLUIDO EN EL PAA		PRESUPUESTO
					ENERO				FEBRERO				MARZO				ABRIL				MAYO				JUNIO				JULIO				AGOSTO				SEPTIEMBRE				OCTUBRE				NOVIEMBRE				DICIEMBRE						SI	NO	
					sem 1	sem 2	sem 3	sem 4	sem 1	sem 2	sem 3	sem 4	sem 1	sem 2	sem 3	sem 4	sem 1	sem 2	sem 3	sem 4	sem 1	sem 2	sem 3	sem 4	sem 1	sem 2	sem 3	sem 4	sem 1	sem 2	sem 3	sem 4	sem 1	sem 2	sem 3	sem 4	sem 1	sem 2	sem 3	sem 4	sem 1	sem 2	sem 3	sem 4	sem 1	sem 2	sem 3	sem 4	sem 1	sem 2	sem 3	sem 4					
		Ejecutar el monitoreo del 100% de los riesgos de Seguridad y privacidad de la información identificados en la entidad	Monitorear los riesgos de Seguridad y privacidad de la información identificados en la entidad	(numero de riesgos de Seguridad y privacidad de la información a los que se les realizo monitoreo / Total de riesgos de Seguridad y privacidad de la información identificados en la entidad)*100																																															**Líder de planeación líder de sistemas**	Informe monitoreo de mapa de riesgos			

Elaboró FIRMADO EN ORIGINAL
Yeiler Eduardo Bernal Gutiérrez
Líder de sistemas

Revisó FIRMADO EN ORIGINAL
Oscar Dario Soler Morales
Líder de Planeación

Sheyla Fanory Caicedo Rincón
Gerente