PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2022

CONTROL DE CAMBIOS

No. VERSIÓN	DESCRIPCIÓN DEL CAMBIO	FECHA
01	Elaboración y emisión del Diagnostico	

	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

INTRODUCCIÓN

En el Decreto 2106 de 2019, en el parágrafo del artículo 16 indica “las autoridades deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones”.

Es así, que el Decreto 1078 de 2015 en el artículo 2.2.9.1.2.2, establece los instrumentos para implementar la Estrategia de Gobierno en Línea, y uno de estos se encuentra la formulación e implementación del Plan de Seguridad y Privacidad de la Información dado que remite al Manual de Gobierno Digital.

El Decreto 1078 de 2015, con el cual se Reglamenta el Sector de Tecnologías de la Información y las Comunicaciones” Define la seguridad de la información como principio de la Política de Gobierno Digital, de igual manera en el artículo 2.2.9.1.2.1 define la estructura de los Elementos de la Política de Gobierno Digital a través de componentes y habilitadores transversales los cuales son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital.

El documento denominado Plan de Seguridad y Privacidad de la Información, expedido por el Ministerio de Tecnologías de Información y de las Comunicaciones, expresa que la adopción del mismo, por las entidades del Estado, conduce a la preservación de la confidencialidad, integridad y disponibilidad de la información, apoyada en un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de la información.

La planificación e implementación del Plan de Seguridad y Privacidad de la Información, en el HOSPITAL REGIONAL DE SOGAMOSO E.S.E está determinado por las necesidades, objetivos, los requisitos de seguridad, los procesos misionales, el tamaño y estructura de la Entidad.

2. OBJETIVOS

2.1 General

Estructurar, documentar y sensibilizar el Plan de Seguridad y Privacidad de la Información, según las normas que lo soporten, con el fin de preservar la confidencialidad, integridad y disponibilidad de la información del HOSPITAL REGIONAL DE SOGAMOSO E.S.E.

2.2 Específicos

1. Actualizar la política de seguridad y privacidad de la información implementada en la institución.
2. Documentar el inventario de activos de información.
3. Promover el uso de mejores prácticas de seguridad de la información en la Institución.
4. Realizar el diagnóstico y estrategia para transición de IPv4 a IPv6
5. Sensibilización y capacitación al personal de planta y líderes del proceso del HOSPITAL REGIONAL DE SOGAMOSO E.S.E en los temas referente a seguridad y privacidad de la información.

3. ALCANCE

Implementar el Plan de Seguridad y Privacidad de la Información en el HOSPITAL REGIONAL DE SOGAMOSO E.S.E de acuerdo con los objetivos establecidos, con el fin de mejorar las prácticas de confidencialidad, integridad, disponibilidad y privacidad de la información relacionada con funcionarios y usuarios.

4. NORMATIVIDAD

4.1. Definiciones

Acceso a la información pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

Activo: Son todo aquellos recursos o componentes de la institución, tanto físico (tangibles), como lógicos (intangibles) que constituyen su infraestructura, patrimonio, conocimiento y reputación en el mercado.

Activo de información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia.
También se puede entender como la institución que esta al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización (ISO/IEC27000)

Análisis de riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel del riesgo (ISO/IEC27000)

Autorización: Consentimiento previo, expreso e informado del titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)

Bases de datos personales: Conjunto organizado de datos personales que sea objeto de tratamiento (Ley 1581 de 2012, art 3)

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética (CONPES 3701)

Criterios del riesgo: Termino de referencia frente a los cuales la importancia de un riesgo se evalúa.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Datos: Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos.

Datos abiertos: Son todos aquellos datos primarios o con sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)

Datos personales: Cualquier información vinculada a que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3)

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información -SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001 (ISO/IEC 27000)

Disponibilidad: Característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

Encargado del tratamiento de datos: Persona natural o jurídica, pública o privada, que por si misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento (Ley 1581 de 2012, art 3)

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

Evaluación del riesgo: Proceso de comparación de los resultados del análisis de riesgo, para evaluar, y determinar su magnitud o si son aceptables o tolerables.

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información (ISO/IEC 27000).

Ley de Habeas Data: Se refiere a la Ley Estatutaria 1266 de 2008.

Ley de Transparencia y Acceso a la información pública: Se refiere a la Ley Estatutaria 1712 de 2014.

Monitoreo: Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de control o las diferentes auditorias de los sistemas integrados de gestión.

Mecanismos de protección de datos personales: Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimizarían o cifrado.

Nivel del riesgo: Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la clasificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma (ISO/IEC 27000).

Política de la seguridad de la información: Es el componente principal para la puesta en marcha del modelo de seguridad y privacidad de la información, y unos de los requisitos del Sistema de Gestión de Seguridad de la Información, es el documento que contiene objetivo, aplicabilidad, alcance, principios, nivel de cumplimiento, fundamentos, roles y responsabilidades que se requieren como requisito para la implementación del sistema de gestión de la seguridad de la información.

Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o este en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Registro Nacional de Bases de Datos: Directorio público de las bases de datos sujetas a tratamiento que operan en el país (Ley 1581 de 2012, art 25).

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias (ISO/IEC 2700).

Seguridad: Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que, en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una

organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua (ISO/IEC 27000).

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas (ISO/IEC 27000).

4.2. Marco Normativo

- Resolución 3564 de 2015, reglamenta aspectos relacionados con la Ley de Transparencia y acceso a la información pública.
- Decreto reglamentario único 1081 de 2015, reglamento sobre la gestión de la información pública.
- Decreto 1078 de 2015, decreto único reglamentario del sector de tecnologías de la información y las comunicaciones.
- Ley 1712 de 2014, Ley de transparencia y acceso a la información pública.
- Acuerdo 03 de 2015 del Archivo General de la nación, lineamientos generales sobre la gestión de documentos electrónicos.
- Ley Estatutaria 1581 de 2012, protección de datos personales.
- Ley 1266 de 2008, disposiciones generales de habeas data y se regula el manejo de la información.

5. DESARROLLO DEL PLAN O PROGRAMA

La implementación del plan de seguridad y privacidad de la información, toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar), el modelo MSPI del Ministerio

de Tecnologías de la información y las Comunicaciones, el modelo integrado de planeación y gestión MIPG y la norma ISO 27001:2018.

5.1 Fase de Diagnostico:

Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.
Determinar el nivel de madurez de los controles de seguridad de la información.
Identificar el avance de la implementación del ciclo de operación al interior de la entidad.
Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.
Identificación del uso de buenas prácticas en ciberseguridad.

5.2 Fase de planificación:

De acuerdo con los resultados de la etapa anterior, se procede a elaborar el plan de seguridad y privacidad de la información alineado con el objetivo misional de la Institución, con el propósito de definir acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo.
El alcance del MSPI permite al Hospital Regional de Sogamoso E.S.E definir los límites sobre los cuales se implementará la seguridad y privacidad. Este enfoque es por procesos y debe extenderse a toda la institución. Para desarrollar el alcance y los límites del modelo se deben tener en cuenta las siguientes recomendaciones: procesos que impactan directamente la consecución de objetivos misionales, procesos, servicios, sistemas de información, ubicaciones físicas, terceros relacionados, e interrelaciones del Modelo de procesos.

5.3 Fase de implementación:

Esta fase le permitirá al Hospital, llevar a cabo la implementación de la planificación realizada en fase anterior del MSPI.

5.4 Fase de evaluación de desempeño:

El proceso de seguimiento y monitoreo del MSPI se hace con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas.

5.5 Fase de mejora continua:

En esta fase el Hospital debe consolidar los resultados obtenidos de la fase de la evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.

6. LÍNEAS DE ESTRATEGIAS DEL PLAN E INDICACIONES.

Fortalecer a un nivel optimizado, controles del sistema de gestión de la información.

- Componente GEL: TIC para la gestión.
- Dominios del marco TI: Servicios tecnológicos, uso y apropiación.
- Objetivo estratégico institucional: Garantizar un sistema de información integral, eficiente y eficaz.

Implementar estrategias de sensibilización en seguridad de la información.

- Componente GEL: TIC para la gestión.
- Dominios del marco TI: Servicios tecnológicos, uso y apropiación.
- Objetivo estratégico institucional: Garantizar un sistema de información integral, eficiente y eficaz.

Indicadores:

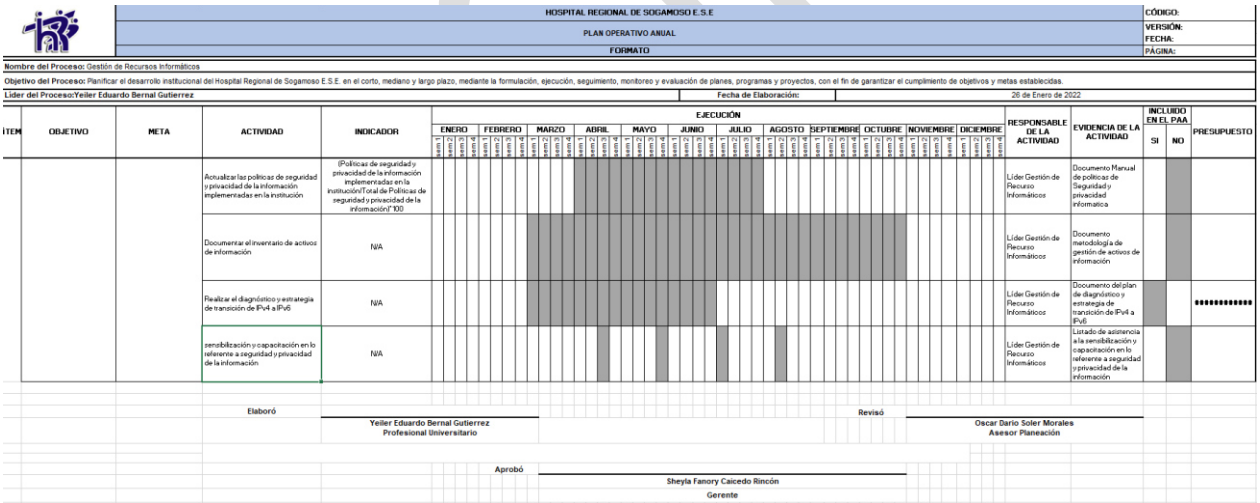
Porcentaje de ejecución de las actividades de ejecución del plan de la vigencia 2022.

Formula: (N° de actividades ejecutadas / N° de actividades programadas) * 100.
Frecuencia de medición: Semestral

7. PLAN DE SEGUIMIENTO.

El seguimiento del presente plan será verificado conforme a lo establecido en el Plan al Operativo Anual 2022 (Plan de Seguridad y Privacidad de la Información).

8. CRONOGRAMA DE EJECUCIÓN.



HOSPITAL REGIONAL DE SOGAMOSO E.S.E	CÓDIGO:
PLAN OPERATIVO ANUAL	VERSIÓN:
FORMATO	FECHA:
	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.

Lider del Proceso: Yeiler Eduardo Bernal Gutierrez — **Fecha de Elaboración:** 26 de Enero de 2022

ÍTEM	OBJETIVO	META	ACTIVIDAD	INDICADOR	EJECUCIÓN (ENERO – DICIEMBRE)	RESPONSABLE DE LA ACTIVIDAD	EVIDENCIA DE LA ACTIVIDAD	INCLUIDO EN EL PAA: SI	INCLUIDO EN EL PAA: NO	PRESUPUESTO
			Actualizar las políticas de seguridad y privacidad de la información implementadas en la institución	(Políticas de seguridad y privacidad de la información implementadas en la institución/Total de Políticas de seguridad y privacidad de la información)*100		Líder Gestión de Recurso Informáticos	Documento Manual de políticas de Seguridad y privacidad informatica			
			Documentar el inventario de activos de información	N/A		Líder Gestión de Recurso Informáticos	Documento metodología de gestión de activos de información			
			Realizar el diagnóstico y estrategia de transición de IPv4 a IPv6	N/A		Líder Gestión de Recurso Informáticos	Documento del plan de diagnóstico y estrategia de transición de IPv4 a IPv6			**********
			sensibilización y capacitación en lo referente a seguridad y privacidad de la información	N/A		Líder Gestión de Recurso Informáticos	Listado de asistencia a la sensibilización y capacitación en lo referente a seguridad y privacidad de la información			

Elaboró: Yeiler Eduardo Bernal Gutierrez — Profesional Universitario

Revisó: Oscar Dario Soler Morales — Asesor Planeación

Aprobó: Sheyla Fanory Caicedo Rincón — Gerente

Ver Plan Operativo Anual 2022.

9. OPORTUNIDAD DE MEJORA.

Los riesgos que se identifiquen durante la ejecución del plan de seguridad y privacidad de la información deberán ser mitigados y monitoreados constantemente, además se deberán actualizar los recursos tecnológicos y activos de información de la entidad de manera regular y cuando se requiera.

	HOSPITAL REGIONAL DE SOGAMOSO E.S.E	CÓDIGO: D-PI-FT-001
	PLAN OPERATIVO ANUAL	VERSIÓN: 02
	FORMATO	FECHA: 30/12/2020
		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 Gutiérrez | **Fecha de Elaboración:** | **26/01/2022**

ÍTEM	OBJETIVO	META	ACTIVIDAD	INDICADOR	EJECUCIÓN	RESPONSABLE DE LA ACTIVIDAD	EVIDENCIA DE LA ACTIVIDAD	INCLUIDO EN EL PAA		PRESUPUESTO
					ENERO: sem 1, sem 2, sem 3, sem 4 / FEBRERO: sem 1, sem 2, sem 3, sem 4 / MARZO: sem 1, sem 2, sem 3, sem 4 / ABRIL: sem 1, sem 2, sem 3, sem 4 / MAYO: sem 1, sem 2, sem 3, sem 4 / JUNIO: sem 1, sem 2, sem 3, sem 4 / JULIO: sem 1, sem 2, sem 3, sem 4 / AGOSTO: sem 1, sem 2, sem 3, sem 4 / SEPTIEMBRE: sem 1, sem 2, sem 3, sem 4 / OCTUBRE: sem 1, sem 2, sem 3, sem 4 / NOVIEMBRE: sem 1, sem 2, sem 3, sem 4 / DICIEMBRE: sem 1, sem 2, sem 3, sem 4			SI	NO	
1	Administrar el nivel de seguridad y privacidad y definir las acciones a implementar en el Hospital Regional de Sogamoso E.S.E.	Proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada.	Actualizar la política de seguridad y privacidad de la información	Política Actualizada		**Líder Gestión de Recurso Informáticos**	Documento Manual de políticas de Seguridad y privacidad informática			
			Actualizar el inventario de activos de información	inventario de activos de información		**Líder Gestión de Recurso Informáticos**	Documento metodología de gestión de activos de información			
			Realizar el diagnóstico y estrategia de transición de IPv4 a IPv6	diagnóstico y estrategia de transición de IPv4 a IPv6		**Líder Gestión de Recurso Informáticos**	Documento del plan de diagnóstico y estrategia de transición de IPv4 a IPv6			$ 50.000.000,00
			sensibilización y capacitación en lo referente a seguridad y privacidad de la información	(colaboradores capacitados / colaboradores de la institución) * 100		**Líder Gestión de Recurso Informáticos**	Listado de asistencia a la sensibilización y capacitación en lo referente a seguridad y privacidad de la información			

Elaboró FIRMADO EN ORIGINAL
Yeiler Eduardo Bernal Gutiérrez
Líder Oficina de Sistemas

Revisó FIRMADO EN ORIGINAL
Oscar Darío Soler Morales
Líder de Planeación

Aprobó FIRMADO EN ORIGINAL
Sheyla Fanory Caicedo Rincón
Gerente