PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

TABLA DE CONTENIDO

1. OBJETIVO

1.1. GENERAL

Definir acciones a seguir para implementar el Modelo de Seguridad y Privacidad de la Información en la ESE IMSALUD propuesto por el MINTIC, que permitirá contribuir a la seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios en la entidad.

1.2. ESPECÍFICOS

- Cumplir con las leyes, regulaciones y obligaciones sectoriales aplicables a la Seguridad de la Información.
- Establecer un cronograma basado en el ciclo de mejora continua para la adopción integral del Modelo de Seguridad y Privacidad de la Información.
- Definir estrategias que permitan realizar seguimiento al Plan de tratamiento de riesgos de seguridad y privacidad de la información.
- Establecer lineamientos para la implementación de mejores prácticas de seguridad que oriente y obligue al uso adecuado de los recursos informáticos.

2. ALCANCE Y LIMITACIONES

El Plan de Seguridad y Privacidad de la Información es aplicado a todos los procesos de la entidad, sus funcionarios, contratistas, proveedores, operadores y aquellas personas o terceros que en razón del cumplimiento de sus funciones y las de la entidad compartan, utilicen, recolecten, procesen, intercambien o consulten su información, englobando todas las sedes físicas de la ESE IMSALUD, así como a los Entes de Control, Entidades relacionadas que accedan, ya sea interna o externamente a cualquier tipo de información, independientemente de su ubicación, iniciando desde la Política de Seguridad y Privacidad de la información hasta la implementación de controles definidos para mitigar los riesgos de seguridad informática definidos en la matriz de riesgos de la entidad.

3. RESPONSABILIDADES

El profesional especializadlo de seguridad y privacidad de la información o en su ausencia el jefe de oficina de Información, sistemas y procesos de la entidad será el encargado de dar continuidad a las actividades descritas en este plan.

4. MARCO NORMATIVO

Constitución Política. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data; Artículo 20. Libertad de Información.

Ley 594 de 2000. “Ley General de Archivo”

Ley 1273 de 2009 Por medio de la cual se modifica el Código Penal. Título VII Bis “De la protección de la información y de los datos”. Artículos 269A a 269J.

Ley 1581 de 2012 Por la cual se dictan disposiciones generales para la protección de datos personales.

Ley 1712 de 2014 Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

Decreto 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 comunicaciones.

CONPES 3854 – 2016 Política Nacional de Seguridad Digital.

5. MARCO CONCEPTUAL

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.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. (ISO/IEC 27000)

Datos Abiertos: Son todos aquellos datos primarios o 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 o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. (ISO/IEC 27000).

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño

a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).
Integridad: Propiedad de la información relativa a su exactitud y completitud. (ISO/IEC 27000).

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, anonimización o cifrado.

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).

Titulares de la información: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)

Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

6. GENERALIDADES DEL DESARROLLO DE LA TEMÁTICA

El proceso de Gestión de Tecnologías de la Información es uno de los principales artífices para lograr el desarrollo del Modelo de Seguridad y Privacidad de la Información en la entidad, el cual permitirá favorecer continuamente la seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios en la entidad, por medio de la definición de políticas, programas, lineamientos, estrategias y actividades.

6.1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La E.S.E. IMSALUD cuenta con una política de seguridad y privacidad de la Información la cual fue adoptada en su versión 04 mediante Resolución No.835 de 2.025 cuya declaratoria es; la E.S.E IMSALUD, gestiona sus activos de información promoviendo su confidencialidad, integridad y disponibilidad dando cumplimiento a la legislación vigente.

6.2. OPERACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El Sistema de Gestión de Seguridad de la Información se encuentra alineado al desarrollo del Modelo Integrado de Gestión, el cual en sus políticas contempla las de Gobierno y Seguridad Digital, Servicio al ciudadano, racionalización de trámites, Participación Ciudadana en la Gestión Pública, transparencia, entre otras.

7. ACCIONES O FASES

No.	ACTIVIDAD	DESCRIPCIÓN	PRODUCTO	FECHA INICIO	FECHA FIN	RESPONSABLE
1	Realizar encuesta de percepción a colaboradores sobre aspectos de seguridad y privacidad de la información	Formular y aplicar una encuesta de percepción sobre la apropiación que tienen los colaboradores frente a aspectos de seguridad y privacidad de la información	Encuesta vía correo electrónico	1/02/2026	28/02/2025	Contratista de Seguridad y Privacidad de la Información
2	Realizar informe de resultados de la encuesta de percepción	En un informe describir y analizar los resultados obtenidos.	Presentar un informe con los resultados de la encuesta.	1/02/2026	28/02/2026	Todos los procesos / Gestión Documental / Contratista de Seguridad y Privacidad de la Información
3	Capacitar sobre seguridad y privacidad de la información, y buenas prácticas a los colaboradores de la entidad	Realizar jornadas de capacitación a los colaboradores de la entidad en temáticas de seguridad y privacidad de la información(SPI), actualizar el curso de SPI en el aula virtual.	Actas y/o Listados de asistencia, reportes de formación virtual. Presentar un informe final con el resultado de las capacitaciones en la vigencia.	1/03/2026	31/12/2026	Contratista de Seguridad y Privacidad de la Información
4	Toma de conciencia - estrategias de apropiación, fondos de escritorio.	Definir estrategias de concientización hacia los colaboradores, así como la realización del curso virtual en seguridad y privacidad de la información. Proyección de piezas gráficas para despliegue en los fondos de escritorio, salvapantallas de los equipos de cómputo de la entidad, además de material para redes sociales de la entidad(Fechas conmemorativas)	Presentar dos informes en la vigencia con los resultados de las estrategias de concientización, tales como piezas gráficas y/o audiovisuales que contengan consejos para buenas prácticas de seguridad y privacidad de la información, que serán desplegadas y compartidas a todo el personal.	1/03/2026	31/12/2026	Contratista de Seguridad y Privacidad de la Información
5	Actualización de levantamiento de activos de información	Actualizar los activos asociados con información por proceso y dependencia en la Entidad	Matriz de registro de activos de información actualizada	1/03/2026	30/04/2026	Contratista de Seguridad y Privacidad de la Información
6	Realizar la identificación y/o actualización de riesgos de seguridad de la información y definir su estado	Se debe realizar la identificación de riesgos de seguridad de la información, definir su nivel y opciones de tratamiento	Matriz con riesgos de seguridad de la información identificados y valorados	1/05/2026	31/05/2026	Contratista de Seguridad y Privacidad de la Información

No.	ACTIVIDAD	DESCRIPCIÓN	PRODUCTO	FECHA INICIO	FECHA FIN	RESPONSABLE
7	Definir el tratamiento de los riesgos	Definir actividades para el tratamiento de riesgos y elaborar cronograma de cumplimiento.	Matriz con riesgos de seguridad y privacidad de la información con actividades para su tratamiento.	1/05/2026	31/05/2026	Contratista de Seguridad y Privacidad de la Información
8	Actualizar la guía de rotulación de la información	Se debe validar con el equipo de archivo y gestión documental, la implementación de procedimientos para el etiquetado de la información de acuerdo con el esquema de clasificación de la información adoptado por la organización, y de ser necesario generar la actualización.	Documento guía para la implementación de la rotulación de la información física y digital según su nivel de clasificación: Pública, Clasificada, Reservada	1/06/2026	30/06/2026	Contratista de Seguridad y Privacidad de la Información / Personal de soporte técnico
9	Aplicar análisis de vulnerabilidades de seguridad digital para los servicios; portal Web, sede electrónica, servicios expuestos en Internet, activos de información conectados a la red en su infraestructura On Premise.	Establecer la aplicación de escaneos de vulnerabilidades trimestrales para identificar y dar solución a debilidades de seguridad informática en los sistemas, redes y aplicativos de la entidad.	Un informe trimestral del desarrollo de escaneos de vulnerabilidades con las respectivas especificaciones y recomendaciones ante los hallazgos encontrados. Total, cuatro informes en la vigencia.	1/01/2026 01/04/2026 01/07/2026 01/10/2026	31/03/2026 30/06/2026 30/09/2026 31/12/2026	Contratista de Seguridad y Privacidad de la Información / Profesional de mesa de ayuda responsable de seguridad perimetral / Personal de soporte técnico
10	Realización de pruebas de continuidad de las TIC	La preparación de las TIC debe planificarse, implementarse, mantenerse y probarse en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC, Realizando pruebas de recuperación de cada uno de los sistemas de información críticos, se podrá determinar el nivel de resiliencia ante posibles irrupciones informáticas.	Un informe en la vigencia que describa las pruebas realizadas y documentadas en todas sus fases que incluya cronograma, fotometría. Mínimo una prueba en la vigencia.	1/08/2026	30/09/2026	Contratista de Seguridad y Privacidad de la Información
11	Realizar pruebas de respaldo a las copias de seguridad de la información de los aplicativos	Se debe identificar la información sensible que requiere salvaguarda a través de Backup, tanto de servidores como de	Un Informe en la vigencia que describa el procedimiento de pruebas de respaldo	1/10/2026	30/11/2026	Contratista de Seguridad y Privacidad de la Información

No.	ACTIVIDAD	DESCRIPCIÓN	PRODUCTO	FECHA INICIO	FECHA FIN	RESPONSABLE
	misionales, estratégicos, soporte y de mejora, de manera programada para asegurar la disponibilidad de los datos en caso de Ransomware, de manera coordinada con los responsables del proceso.	máquinas virtuales, valorando su grado de criticidad y estableciendo la periodicidad en la que se desarrollará y el tiempo necesario de almacenamiento de acuerdo a los recursos tecnológicos existentes en la entidad.	de las copias de seguridad.			
12	Verificación cumplimiento de firma de acuerdos de confidencialidad y tratamiento de datos personales	Validar el cumplimiento de la firma de los acuerdos de confidencialidad y tratamiento de datos personales, en los procesos de contratación, gestión de identidades y demás procesos que requieran de la firma de los acuerdos.	Informe trimestral de verificación de cumplimiento de los acuerdos. Cuatro informes en la vigencia.	1/01/2026 1/04/2026 1/07/2026 1/10/2026	31/03/2026 30/06/2026 30/09/2026 31/12/2026	Contratista de Seguridad y Privacidad de la Información / Profesional de mesa de ayuda responsable de seguridad perimetral / Personal de soporte técnico
13	Reportar los incidentes de seguridad digital de la entidad, acorde con lo establecido en la Resolución 500 de 2021.	Gestionar los incidentes de seguridad digital, para realizar el tratamiento, investigación y gestión de los incidentes asociados a los activos de información de la entidad en cada proceso. Y se deberá reportar ante el CSIRT (Equipo de Respuesta a Incidentes de Seguridad Digital) a través del formato de reporte establecido por el CSIRT Gobierno nacional.	Un Informe trimestral que contenga la descripción de cada uno de los incidentes y/o novedades presentadas, y el resultado en la gestión de incidentes de seguridad digital. Cuatro informes en la vigencia.	1/01/2026	31/12/2026	Contratista de Seguridad y Privacidad de la Información / Personal de soporte técnico/ jefe dependencia
14	Realizar análisis y seguimiento a los incidentes de seguridad digital presentados	La organización debe evaluar los eventos de seguridad de la información, su remediación y lecciones aprendidas.	Un Informe trimestral que indique si se presentaron incidentes de seguridad digital, y se defina del total de incidentes presentados y el tratamiento oportuno. Cuatro informes en la vigencia.	1/01/2026	31/12/2026	Contratista de Seguridad y Privacidad de la Información

No.	ACTIVIDAD	DESCRIPCIÓN	PRODUCTO	FECHA INICIO	FECHA FIN	RESPONSABLE
15	Mantener actualizados los indicadores de seguridad y privacidad de la información.	Mantener actualizados los indicadores de seguridad y privacidad de la información, revisando periódicamente los datos que reflejan el estado de la gestión institucional, actualizarlos en los tableros de control en Almera.	Reportes de actualización de indicadores de seguridad y privacidad de la información mensual y trimestral según corresponda.	1/01/2026	31/12/2026	Contratista de Seguridad y Privacidad de la Información
16	Actualización instrumento de evaluación MSPI	Actualizar el instrumento MSPI de MinTIC en la entidad, valorando cada dominio de la norma ISO 27001:2013	Archivo Excel con instrumento MSPI actualizado.	1/11/2026	30/11/2026	Contratista de Seguridad y Privacidad de la Información/ equipo de prensa

8. RECURSOS

Para el desarrollo del Plan de seguridad y privacidad de la Información la entidad invertirá recursos propios, con la asignación de un profesional especializado en seguridad y privacidad de la información que desarrollará las actividades definidas en concordancia con la metodología e involucrando a los diferentes líderes de proceso.

9. TIEMPO DE EJECUCIÓN

Para el desarrollo de las actividades del plan de seguridad y privacidad de la información se requiere de la aplicación de actividades continúas establecidas para ejecutarse en el periodo comprendido entre el 1 de enero y el 31 de diciembre de 2026, cumpliendo con cada uno de los tiempos establecidos en las acciones y fases del plan.

10. EVALUACIÓN

La evaluación del presente plan se realizará a través del indicador:

Cumplimiento del Plan de Seguridad y privacidad de la información: Actividades cumplidas en el período / cantidad de actividades programadas en el período.

11. PLAN DE ACCIÓN

Objetivo:	Definir acciones a seguir para implementar el Modelo de Seguridad y Privacidad de la Información en la ESE IMSALUD propuesto por el MINTIC, que permitirá contribuir a la seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios en la entidad.													
Número de Actividad	**Descripción de la actividad**	**Responsable**	**AÑO 2025**											
			EN	FE	MA	AB	MA	JU	JL	AG	SE	OC	NO	DI
1	Realizar encuesta de percepción a colaboradores sobre aspectos de seguridad y privacidad de la información	Contratista de Seguridad y Privacidad de la Información		x										
2	Realizar informe de resultados de la encuesta de percepción	Todos los procesos / Gestión Documental / Contratista de Seguridad y Privacidad de la Información		x										
3	Capacitar sobre seguridad y privacidad de la información, y buenas prácticas a los colaboradores de la entidad	Contratista de Seguridad y Privacidad de la Información			x	x	x	x	x		x	x	x	x
4	Toma de conciencia - estrategias de apropiación, fondos de escritorio.	Contratista de Seguridad y Privacidad de la Información			x	x	x	x	x	x	x	x	x	x
5	Actualización de levantamiento de activos de información	Contratista de Seguridad y Privacidad de la Información			x	x								
6	Realizar la identificación y/o actualización de riesgos de seguridad de la información y definir su estado	Contratista de Seguridad y Privacidad de la Información					x							
7	Definir el tratamiento de los riesgos	Contratista de Seguridad y Privacidad de la Información					x							
8	Actualizar la guía de rotulación de la información	Contratista de Seguridad y Privacidad de la Información / Personal de soporte técnico						x						
9	Aplicar análisis de vulnerabilidades de seguridad digital para los servicios; portal Web, sede electrónica, servicios expuestos en Internet, activos de información conectados a la red en su infraestructura On Premise.	Contratista de Seguridad y Privacidad de la Información / Profesional de mesa de ayuda responsable de seguridad perimetral / Personal de soporte técnico			X			X			X			x
10	Realización de pruebas de continuidad de las TIC	Contratista de Seguridad y Privacidad de la Información								x	x			
11	Realizar pruebas de respaldo a las copias de seguridad de la información de los aplicativos misionales, estratégicos, soporte y de mejora, de manera programada para asegurar la disponibilidad de los datos en caso de Ransomware, de manera coordinada con los responsables del proceso.	Contratista de Seguridad y Privacidad de la Información										X	X	
12	Verificación cumplimiento de firma de acuerdos de confidencialidad y tratamiento de datos personales	Contratista de Seguridad y Privacidad de la Información / Profesional de mesa de ayuda responsable de			x			x			x			x

Objetivo:	Definir acciones a seguir para implementar el Modelo de Seguridad y Privacidad de la Información en la ESE IMSALUD propuesto por el MINTIC, que permitirá contribuir a la seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios en la entidad.												
Número de Actividad	**Descripción de la actividad**	**Responsable**	**AÑO 2025**										
			EN	FE	MA	AB	MA	JU	JL	AG	SE	OC	NO	DI
		seguridad perimetral / Personal de soporte técnico												
13	Reportar los incidentes de seguridad digital de la entidad, acorde con lo establecido en la Resolución 500 de 2021.	Contratista de Seguridad y Privacidad de la Información / Personal de soporte técnico/ jefe dependencia	x	x	x	x	x	x	x	x	x	x	x	x
14	Realizar análisis y seguimiento a los incidentes de seguridad digital presentados	Contratista de Seguridad y Privacidad de la Información	X	X	X	X	X	X	X	X	X	X	X	X
15	Mantener actualizados los indicadores de seguridad y privacidad de la información.	Contratista de Seguridad y Privacidad de la Información	x	x	x	x	x	x	x	x	x	x	x	x
16	Actualización instrumento de evaluación MSPI	Contratista de Seguridad y Privacidad de la Información/ equipo de prensa											x	

12. HISTORIAL DE CONTROL DE CAMBIOS

VERSIÓN	MOTIVO	FECHA
01	Elaboracion del Plan	2020
02	Actualizacion del Plan	2021
03	Actualizacion del Plan con la estructura documental	27/01/2022
04	Actualización del cronograma vigencia 2023	25/01/2023
05	Actualización del cronograma vigencia 2024	25/01/2024
06	Actualizacion de alcance, responsabillidades, política, acciones o fases, recursos, tiempo de ejecución, plan de acción vigencia 2025	28/01/2024
07	Actualización capítulos de la política SPI, acciones o fases, tiempos de ejecución, y plan de acción	27/01/2026
08		

Elaboró:	Revisó:	Aprobó:
Profesional Especializado en Seguridad y Privacidad de la Información.	Jefe de Información Sistemas y Procesos	Comité Institucional de Gestión y Desempeño