Tabla de contenido

1. Introducción

El sector salud enfrenta desafíos únicos en protección de datos, donde la información clínica se convierte en un activo crítico que requiere salvaguardas especiales. Este plan establece lineamientos para garantizar la **confidencialidad, integridad y disponibilidad** de la información en el Hospital Departamental María Inmaculada ESE, con especial énfasis en datos de salud y personales. Surge como respuesta a:

- Incremento de ciberamenazas al sector salud
- Exigencias de la **Ley 1581 de 2012** y **Resolución 1995 de 1999**
- Necesidad de estandarizar prácticas de seguridad según **ISO 27001**

Este plan integral establece un marco estratégico y operativo para garantizar la protección de:

- **Datos sensibles de pacientes** (historias clínicas, diagnósticos, imágenes médicas)
- **Información operativa crítica** (suministros médicos, infraestructura tecnológica)
- **Datos personales** (empleados, familiares, proveedores)

Contexto actual: Los hospitales colombianos enfrentan un aumento del 217% en ciberataques (Fuente: CSIRT-Gob 2023), siendo el ransomware y el robo de historias clínicas las principales amenazas. Este plan se alinea con:

- El Marco de Ciberseguridad para el Sector Salud (Minsalud 2022)
- La Estrategia Nacional de Seguridad Digital (MINTIC 2023)
- Los estándares internacionales para interoperabilidad segura en salud (HL7 FHIR)

De esta manera, la Seguridad de la Información es una prioridad para el Hospital departamental María Inmaculada ESE, y por tanto es responsabilidad de todas las partes interesadas cumplir con el presente plan y velar por que no se realicen actividades que contradigan la esencia y el espíritu de cada una de las políticas contenidas en dicho documento.

2. Objetivo

Planear e implementar las estrategias para la gestión de seguridad y privacidad de la Información en el Hospital Departamental María Inmaculada ESE, que permitan minimizar los riesgos de pérdida de activos de la información, alineadas a las directrices emanadas por MinTIC y acordes con las necesidades del hospital.

2.1. Objetivos Específicos

- Disminuir la probabilidad de ocurrencia e impacto de los incidentes de Seguridad y Privacidad de la Información de forma efectiva.
- Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad, autenticidad, y privacidad de la información del Hospital Departamental María Inmaculada ESE.
- Asegurar y hacer uso eficiente y seguro de los recursos de Tecnologías de Información y Comunicaciones, con el fin de garantizar la continuidad de la prestación de los servicios.
- Dar cumplimiento a los requisitos legales y normativos en materia de Seguridad y Privacidad de la Información, Seguridad Digital y protección de la información personal.
- Minimizar el riesgo de vulnerabilidad de la información en el desarrollo de los procesos.
- Mantener la confianza de los clientes internos y externos.
- Asegurar la continuidad de funcionamiento de la plataforma informática.
- Cumplir con la legislación nacional e institucional sobre seguridad de la información.
- Garantizar la disponibilidad de la información para la eficiente toma de decisiones.
- Fortalecer la cultura de la seguridad de la información a nivel de clientes internos y externos.
- Proteger los activos tecnológicos y apoyar su desarrollo.

3. Términos y 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:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).
- **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.
- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).
- **Antivirus:** Software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus. El antivirus debe ser parte de una estrategia de seguridad estándar de múltiples niveles.
- **Ataques Web:** Es un ataque que se comete contra una aplicación cliente y se origina desde un lugar en la Web, ya sea desde sitios legítimos atacados o sitios maliciosos que han sido creados para atacar intencionalmente a los usuarios de ésta.
- **Contraseña:** Cadena exclusiva de caracteres que introduce un usuario como código de identificación para restringir el acceso a equipos y archivos confidenciales. El sistema compara el código con una lista de contraseñas y usuarios autorizados
- **Confidencialidad:** Propiedad que determina que la información está disponible ni sea revelada a quien no esté autorizado (2.13 ISO 27000)
- **Disponibilidad:** Propiedad que la información sea accesible y utilizable por solicitud de los autorizados (2.10 ISO 27000).

- **Integridad:** Propiedad de salvaguardar la exactitud y el estado completo de los activos (2.36 ISO 27000).
- **Encriptación:** La encriptación es un método de cifrado o codificación de datos para evitar que los usuarios no autorizados lean o manipulen los datos. Sólo los individuos con acceso a una contraseña o clave pueden descifrar y utilizar los datos.
- **Firewall:** Es una aplicación de seguridad física y/o lógica diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno. Un firewall debería formar parte de una estrategia de seguridad estándar de múltiples niveles.
- **Malware:** Es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras.
- **Plan de tratamiento de Gestión 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).
- **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 esté 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.
- **Procedimiento:** Sucesión cronológica de acciones concatenadas entre sí, para la realización de una actividad o tarea específica dentro del ámbito de los controles de Seguridad de la Información.
- **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 27000).
- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- **Sistema de detección de intrusos:** Es un servicio que monitorea y analiza los eventos del sistema para encontrar y proporcionar en tiempo real o casi real advertencias de intentos de acceso a los recursos del sistema de manera no autorizada. Es la detección de ataques o intentos de intrusión, que consiste en revisar registros u otra información disponible en la red.
- **Virus:** Programa informático escrito para alterar la forma como funciona una computadora, sin permiso o conocimiento del usuario.
- **Vulnerabilidad:** Es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad de los sistemas.

4. Marco normativo o base legal

- **Resolución 1995 de 1999**: Por la cual se establece normas para el manejo de la historia clínica y se establecen la organización y manejo del archivo de historias clínicas, custodia, acceso y seguridad. La entidad como prestadora de servicios de salud, tiene bajo su custodia la información de historia clínica de los pacientes, siendo esta norma de obligatorio cumplimiento para el hospital ya que indica los registros que debe contener, quienes pueden tener acceso a ella, la custodia, la seguridad y condiciones de almacenamiento.
- **Ley 1266 de 2008**: Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Tiene por objeto desarrollar el derecho constitucional de conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en

bancos de datos, además de los derechos, libertades y garantías relacionadas con la recolección, tratamiento y circulación de datos personales, así como el derecho a la información. La entidad como Operador de información, por recibir información de datos personales directamente del titular, tiene la administración de los mismos, por tanto, está obligado a garantizar la protección de estos datos.

- **Ley 1581 de 2012**: Protección de datos personales. Por la cual se dictan disposiciones generales para la protección de datos personales, cuyo objeto es desarrollar el derecho constitucional a conocer, actualizar y rectificar informaciones que se hayan recogido en bases de datos o archivos, así como el derecho a la información consagrado. Sobre el tratamiento de datos personales se aplican diferentes principios, entre ellos, el de transparencia, acceso y circulación restringida, de seguridad y confidencialidad.
- **Decreto 903 de 2014:** Por el cual se dictan disposiciones en relación con el Sistema Único de Acreditación en salud. Dicta disposiciones y realiza ajustes al sistema único de acreditación en Salud, como componente del Sistema Obligatorio de Garantía de Calidad de la Atención de salud. El sistema de acreditación es voluntario, y las entidades que deciden implementarlo, deben comprobar el cumplimiento de niveles de calidad superiores a los requisitos mínimos obligatorios (habilitación)
- **Resolución 3100 de 2019:** Por la cual se define los estándares de habilitación para las instituciones prestadoras de servicios de salud, dentro de ellos Historia Clínica y Registros, que busca la existencia y cumplimiento de procesos que garanticen la historia clínica por paciente y las condiciones técnicas de su manejo y el de los registros de procesos clínicos que se relacionan directamente con los principales riesgos propios de la prestación de servicios, estableciendo que para la gestión de las historias en medios electrónicos, se debe garantizar la confidencialidad y seguridad, sin que se puedan modificar los datos una vez se guarden los registros, garantizando la confidencialidad del documento protegido legalmente por reserva

5. Responsable

- Comité de MIPG: Aprobar políticas y evaluar riesgos.
- Oficina de TI: Supervisar cumplimiento a la protección de datos personales e implementar controles técnicos.
- Jefes de áreas: Garantizar cumplimiento por su personal.

6. Indicadores

- % de incidentes con el sistema de información resueltos en 24h.
  - Numerador: incidentes resueltos.
  - Denominador: total reportados * 100
  - Meta: >=90%
  - Frecuencia: mensual
- Tasa de accesos no autorizados a la página web institucional.
  - Numerador: intentos fallidos
  - Denominador: total accesos
  - Meta: <0.5%
  - Frecuencia: trimestral

7. Estructura documental

La seguridad de la información incluye tres dimensiones principales: la confidencialidad, la disponibilidad y la integridad. Con el objetivo de garantizar el procesamiento sostenido, así como su continuidad, y minimizar impactos, la seguridad de la información conlleva la aplicación y la gestión de medidas de seguridad adecuadas que implican la consideración de una amplia gama de amenazas.

La seguridad de la información se consigue mediante la implementación de un conjunto de controles aplicables, seleccionados a través del proceso de gestión de riesgo que se haya elegido y gestionado por medio de un SGSI, empleando políticas, procesos, procedimientos, estructuras organizativas, software y hardware para proteger los activos de información identificados.

Estos controles necesitan ser especificados, implementados, monitoreados, revisados y mejorados cuando sea necesario, para garantizar que la seguridad y el cumplimiento de la normatividad se cumplan. Estos controles de seguridad de la información deben integrarse de forma coherente con los procesos de la institución. Un gran número de factores son fundamentales para la implementación exitosa de un SGSI que permita a la organización cumplir con sus objetivos.

El Hospital Departamental María Inmaculada ESE viene aumentando la automatización de sus procesos mediante la adquisición de aplicativos externos, tanto en ambiente cliente servidor como en la web.

Estos aplicativos pueden estar expuestos a amenazas, como malware o hacking, entre otros, pero también a riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde cualquier origen o los causados accidentalmente por fallas técnicas y desastres naturales, por lo que se considera de vital importancia la implementación de un SGSI, debido a que este sistema ayuda a la entidad a gestionar de manera eficaz la seguridad de la información, con el objetivo de definir y aplicar medidas, procesos y procedimientos para el apropiado control, tratamiento y mejora continua.

A continuación, se detallan las fases y sus correspondientes actividades que se van a desarrollar teniendo en cuenta lo definido descrito en los lineamientos del documento “Modelo de Seguridad y Privacidad de la Información (MSPI)” del MinTIC alineados con el Marco de Referencia de Arquitectura Empresarial para la Gestión de TI (MRAE), la Estrategia de Gobierno en Línea (GEL) y la Norma Técnica Colombiana NTC-ISO-IEC 27001:2013.

7.1. Fases de implementación del SGSI.

- **FASE I Análisis de brecha:** Elaborar el análisis GAP (análisis de brecha) frente a la norma ISO 27000.
- **FASE II Establecimiento del SGSI:** Diseñar políticas y procedimientos de seguridad conforme la estructura propuesta por la norma ISO 27000 alineados al Sistema Integrado de Gestión de la Entidad. Definir y documentar formalmente el proceso de gestión de incidentes del SGSI Crear, definir e implementar los indicadores (métricas) adecuados para medir la madurez, eficiencia, eficacia, implantación o impacto de controles de seguridad de la información. Se deberá tener como referencia la norma ISO 27004:2016.
- **FASE III Análisis de riesgos:** Actualizar los activos de información de la institución y ajustar su clasificación de acuerdo con los requerimientos de confidencialidad definidos y establecer los requerimientos exigidos por la norma ISO 27001:2013 y normas relacionadas ISO 27002 e ISO

27005. Actualizar el plan de gestión de riesgos de la ESE basados en los lineamientos establecidos en la norma ISO 31000 e ISO 27005:2008, y en la actualización de los activos de información.

- **FASE IV Pruebas de seguridad:** Desarrollo de pruebas para determinar las vulnerabilidades que existen dentro de la configuración física y lógica de la plataforma informática de la entidad. Realización de pruebas de Ingeniería social buscando evidenciar las vulnerabilidades que existen dentro de la ESE, mediante la obtención de información de personas y procesos claves del negocio mediante acceso físico a la misma o con información de acceso facilitada por el personal de la organización, el cual ha sido objeto de engaño. Construir el Plan Estratégico de Seguridad de la Información PESI.
- **FASE V Sensibilización y entrenamiento en seguridad de la información:** Establecer las acciones necesarias para implementar el programa de capacitación requerido por la organización en lo referente a seguridad de la información tomando como insumo los resultados de las pruebas de ingeniería social y a lo definido en el Plan Estratégico de Seguridad de la Información PESI.
- **FASE VI Auditoria interna:** Diseñar y desarrollar las actividades preparatorias que busquen orientar a la organización para afrontar el proceso de auditoría por parte de un ente certificador el cual comprenderá efectuar una revisión y cumplimiento del SGSI frente a los requerimientos exigidos para la certificación ISO 27001:2013.

7.2. Cronograma

Fase / Tiempo	2025	2026	2027
Fase I	II semestre		
Fase II		I semestre	
Fase III		III trimestre	
Fase IV		IV trimestre	
Fase V			I semestre
Fase VI			II semestre

CONTROL DE CAMBIOS		
Versión	**Descripción de cambio**	**Fecha de aprobación**
01	Creación del documento	

Instructivo para diligenciar el formato
"Plantilla de plan"

Objetivo: Estandarizar la plantilla del documento denominado como plan, sosteniendo uniformidad en todos los documentos de la entidad.

Para el diligenciamiento correcto de la plantilla tenga en cuenta lo siguiente:

Encabezado

Nombre del proceso: Registre solo el nombre completo del proceso al que pertenece el documento, sin que anteceda la palabra **proceso**, en Arial 10 en negrita. Este espacio debe ser sombreado con color verde.

Nombre del documento: Corresponde al nombre que se le sea asignado, a este se le debe anteponer el tipo de documento, por ejemplo, programa. En Arial 12 en negrita.

Código: Registre la identificación alfanumérica del documento, donde se debe registrar la abreviatura del proceso al que corresponda el documento, seguido la abreviatura del tipo de documento y por último el número consecutivo, en Arial 10 en negrita.

Nota: *Si el documento es para elaboración el campo de código será diligenciado por el proceso de mejoramiento continuo.*

Tabla de contenido: El presente tipo de documento debe contar con una tabla de contenido. La cual siempre es recomendable elaborarla de último, respetando su posición dentro del documento.

1. Introducción: Utilice el presente espacio para contextualizar el plan y mencionar lo que está expuesto a continuación, estableciendo la importancia del tema o lo más relevante en el documento, y posteriormente las conclusiones.

2. Objetivo: Registre el propósito central de lo que se espera lograr con el plan en términos de conocimiento; este debe dar inicio con un **solo** verbo infinitivo, por ejemplo: desarrollar, establecer, implementar, entre otros.

3. Términos y definiciones: Relacione los términos y/o definiciones que consideren importante resaltar y que serían una ayuda para el entendimiento del documento. Estos términos, definiciones, siglas y demás deben ir organizados alfabéticamente.

4. Marco normativo o base legal: Registre la normatividad vigente que soporta la información documentada.

5. Responsable: Mencione únicamente el o los cargos de los colaboradores, el nombre del proceso y/o servicio/área que son responsables de adherirse a lo consignado en el documento.

6. Indicadores: Registre los indicadores que considere pertinentes para la medición y seguimiento del plan.

7. Estructura documental: Registre toda la información general, detallada y/o especifica que pretende trasmitir con el documento. A partir de este espacio se pueden incluir todas las herramientas, actividades, imágenes (las cuales deben ir etiquetadas, con su respectiva fuente y relacionadas en la tabla de contenido, en los documentos que aplique) tablas y cualquier otro elemento que consideren importantes para la adecuada comprensión del documento, teniendo en cuenta no extralimitarse con información que redunde o realmente no necesaria para el tipo de documento.