PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2026

1. INTRODUCCIÓN

El Plan Institucional de Seguridad y Privacidad de la Información (PISPI) del Hospital Mental de Antioquia – María Upegui (E.S.E. HOMO) constituye un instrumento estratégico orientado a fortalecer la protección de los activos de información, garantizar la continuidad de los procesos misionales y de apoyo, y asegurar el cumplimiento de los objetivos institucionales en el entorno digital.

Este Plan se fundamenta en un enfoque preventivo y de gestión del riesgo, que promueve el desarrollo de una cultura organizacional orientada a la seguridad y privacidad de la información. A partir de la comprensión del contexto institucional, los riesgos asociados al uso de las Tecnologías de la Información y las Comunicaciones (TIC) y las amenazas del entorno digital, se establecen acciones sistemáticas para la identificación, análisis, evaluación, tratamiento y monitoreo de los riesgos que puedan afectar la confidencialidad, integridad, disponibilidad, autenticidad y privacidad de la información.

El PISPI se formula en cumplimiento de la normativa vigente del Estado colombiano, en especial lo dispuesto en el CONPES 3854 de 2016, el Decreto 1008 de 2018, la Resolución 500 de 2021 y el Modelo de Seguridad y Privacidad de la Información (MSPi) del Ministerio de Tecnologías de la Información y las Comunicaciones, así como en alineación con las buenas prácticas del estándar NTC ISO/IEC 27001:2013, la norma ISO 31000:2018 y la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas emitida por el Departamento Administrativo de la Función Pública.

En este sentido, el Plan se concibe como un marco de referencia para la toma de decisiones, la definición de controles, la asignación de responsabilidades y el fortalecimiento de la gestión institucional de la seguridad digital, contribuyendo a la confianza de las partes interesadas y al adecuado cumplimiento de la misión del Hospital.

2. JUSTIFICACIÓN

2.1 La Información como Activo Estratégico

En la E.S.E. Hospital Mental de Antioquia – María Upegui, la información constituye un activo estratégico y de alto valor. No solo sustenta la operación diaria y la toma de decisiones clínicas y administrativas, sino que también contiene datos personales sensibles de pacientes, historias clínicas, registros terapéuticos e información de salud protegida, cuya confidencialidad es un imperativo ético y legal.

2.2 Contexto de Amenazas y Vulnerabilidades

El entorno digital actual presenta amenazas crecientes y sofisticadas (ransomware, phishing, brechas de datos) que exponen a las instituciones de salud a riesgos significativos. Una violación de la seguridad puede resultar en: pérdida de confianza pública, sanciones legales y económicas, interrupción de servicios críticos y, lo más importante, un daño potencial al bienestar de los pacientes.

2.3 Necesidad de un Marco Integral de Protección

Para enfrentar estos desafíos, no es suficiente con implementar soluciones tecnológicas aisladas. Se requiere un marco integral de gobierno y gestión de seguridad, que:

- Identifique y valore todos los activos de información.
- Evalúe y priorice los riesgos de manera objetiva.
- Establezca e implemente controles de seguridad (preventivos, detectivos y correctivos) organizados y medibles.
- Defina roles y responsabilidades claros para toda la organización.
- Fomente una cultura de concienciación y responsabilidad compartida.

2.4 Finalidad del Plan

Por lo tanto, este Plan se justifica como el instrumento rector que permite a la institución transitar de un enfoque reactivo a uno proactivo y sistemático en la protección de su información. Su implementación es fundamental para salvaguardar la reputación institucional, asegurar el cumplimiento normativo y, en última instancia, proteger la misión de cuidado y servicio a la comunidad.

3. OBJETIVO

Definir, implementar y mantener el Plan Institucional de Seguridad y Privacidad de la Información de la E.S.E. Hospital Mental de Antioquia – María Upegui, mediante la adopción de un enfoque de gestión y gobierno de las Tecnologías de la Información y las Comunicaciones, que permita proteger los activos de información, gestionar los riesgos de seguridad digital y dar cumplimiento a los requisitos legales, normativos y técnicos aplicables.

Objetivos Específicos

- Establecer lineamientos claros para la gestión de la seguridad y privacidad de la información generada, procesada, almacenada y transmitida en los diferentes procesos de la Entidad, incluyendo la gestión de activos, el uso aceptable de los recursos tecnológicos, el acceso a internet y correo electrónico, la clasificación de la información y los acuerdos de confidencialidad.

- Definir y fortalecer el gobierno de la seguridad de la información mediante una estructura organizacional formalmente establecida, que permita la adecuada toma de decisiones, la asignación de responsabilidades y la supervisión de las actividades relacionadas con la protección de los activos de información.

- Designar y fortalecer el rol del responsable de la seguridad de la información (CISO o equivalente), encargado de coordinar, supervisar y promover la implementación del Sistema de Gestión de Seguridad de la Información en la Entidad.

- Implementar planes de contingencia, continuidad del negocio y recuperación ante desastres, que permitan reaccionar de manera oportuna, organizada y efectiva frente a incidentes que afecten la operación de los sistemas de información y la prestación de los servicios.

- Reducir la probabilidad de ocurrencia y el impacto de los incidentes de seguridad y privacidad de la información, mediante la aplicación de controles técnicos, administrativos y físicos adecuados.

- Fortalecer la cultura de seguridad de la información en los funcionarios, contratistas, proveedores y terceros, a través de programas de capacitación, sensibilización y reinducción periódica.

- Asegurar el uso eficiente, seguro y confiable de los recursos de TIC y de los equipos biomédicos que gestionan información, garantizando la continuidad de la prestación de los servicios de salud.

- Garantizar la disponibilidad, integridad y confidencialidad de la información para apoyar la toma de decisiones y mantener la confianza de los usuarios internos y externos.

4. MARCO NORMATIVO

NORMA	CONTENIDO
Constitución Política de Colombia 1994 art 15	Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.
PETI institucional	Plan estratégico de tecnología de la información PETI HOMO 2025-2028
Plan de desarrollo	En el Plan de desarrollo 2025 2028 aprobado por la Junta Directiva, se definió en una de las líneas estratégicas 3.3 Administración estratégica Optimización de recursos. 3.3.2 Gestión estratégico de las TICS.
Decreto 612 del 4 de abril de 2018	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado.
Decreto 1008 de 14 de junio de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
Resolución 0093 de 11	Por la cual se delegan unas funciones, se conforman de febrero, unos comités y se dictan otras disposiciones. Título XI – Capítulos Segundo y Tercero
Resolución 500 de marzo 10 de 2021	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital.
Constitución Política de Colombia 1991	Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.
Norma Técnica Colombiana NTC/ISO 27001:2013	Sistemas de Gestión de la Seguridad de la Información.
Modelo de Seguridad y Privacidad de la Información	Ministerio de Tecnologías y Sistemas de Información.
Ley 1266 de 2008	“Por la cual se dictan las 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
Ley 1581 de 2012.	“Por la cual se dictan disposiciones generales para la Protección de Datos Personales”
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “de la protección de la información y

	de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las Comunicaciones, entre otras disposiciones.
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Dentro del contexto organizacional requerido para el desarrollo del PETI en la E.S.E HOMO, como una entidad que administra recursos de interés público es fundamental tener en cuenta la normatividad vigente que define el objetivo misional de las entidades, sus responsabilidades y el desarrollo de algunas de las funciones requeridas para apoyar el cumplimiento de dicho objetivo misional.

5. DEFINICIONES

- **Acción correctiva:** Remediación de los requisitos o acciones que dieron origen al establecimiento de una no conformidad, de tal forma que no se repita.
- **Acción preventiva:** Disposición de operaciones que buscan de forma preliminar, que no se presente en su ejecución, desarrollo e implementación una no conformidad.
- **Aceptación del riesgo:** Después de revisar las consecuencias que puede acarrear un riesgo, se toma la decisión de asumirlo.
- **Activo:** Se entiende información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Es todo activo que contiene información, la cual posee un valor y es necesaria para realizar los procesos misionales y operativos de la Entidad. Se pueden clasificar de la siguiente manera:
- **Datos:** Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en la Entidad.
- **Aplicaciones**: Es todo el software que se utiliza para la gestión de la Información del HOMO, ejemplo SAFIX, SXG5 ADVANCED, SAIA.
- **Personal:** Es todo el personal de la Entidad, el personal subcontratado, los clientes, usuarios y en general, todos aquellos que interactúen de una manera u otra con los activos de información de la Entidad.
- **Servicios:** Son tanto los servicios internos, aquellos que una parte de la organización suministra a otra, como los externos, aquellos que la organización suministra a clientes y usuarios.

- **Tecnología:** Son todos los equipos utilizados para gestionar la Información y las comunicaciones
- **Instalaciones:** Son todos los lugares espaciales donde se alojan los Sistemas De Información.
- **Administración de incidentes de seguridad:** Procedimientos, estrategias y herramientas de control, enfocados a una correcta evaluación de las amenazas existentes, en este caso hacia toda la infraestructura de TI, se basa en un análisis continuo y mejorado del desempeño de todos los activos y recursos gerenciales que tiene la entidad

  Su objetivo principal es atender y orientar las acciones inmediatas para solucionar cualquier situación que cause una interrupción de los diferentes servicios que presta la entidad, de manera rápida y eficaz. No se limita a la solución de problemas específicos sino a buscar las causas que determinaron el incidente limitando el marco de acción de futuras ocurrencias, su enfoque se base en tres pilares fundamentales:
  - Detectar cualquier alteración en los servicios TI.
  - Registrar y clasificar estas alteraciones.
  - Asignar el personal encargado de restaurar el servicio.
- **APT:** (Advance Persistent Threat) Amenaza Avanzada Persistente Especie ciberataque que es responsable del lanzamiento de ataques de precisión y tienen como objetivo comprometer una máquina en donde haya algún tipo de información valiosa.
- **Alcance:** Ámbito de la organización que queda sometido al Sistema de Gestión de Seguridad de la Información – SGSI. Debe incluir la identificación clara de las dependencias, interfaces y límites con el entorno, sobre todo si solo incluye una parte de la organización.
- **Alerta:** Una notificación formal de que se ha producido un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre.
- **Almacenamiento en la nube:** Del inglés Cloud Storage, es un modelo de almacenamiento de datos basado en redes de computadoras que consiste en guardar archivos en un lugar de Internet. Esos lugares son ubicaciones remotas cuya finalidad es ofrecer seguridad a la información o procesos allí alojados.
- **Amenaza:** Según ISO 13335-1:2004; causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o a la organización.
- **Análisis de riesgos:** A partir del riesgo definido, se define las causas del uso sistemático de la información para identificar fuentes y estimar el riesgo.
- **Auditor:** Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.
- **Auditoría:** Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

- **Autenticación:** Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.
- **Autenticidad:** Los activos de información solo pueden estar disponibles verificando la identidad de un sujeto o recurso, es la propiedad que garantiza que la identidad de un sujeto o recurso es la que declara y se aplica a entidades tales como usuarios, procesos, sistemas de información.
- **Base de datos de gestión de configuraciones (CMDB, Configuration Management Database):** Es una base de datos que contiene toda la información pertinente acerca de los componentes del sistema de información utilizado en una organización de servicios de T.I y las relaciones entre componentes. Una CMDB ofrece una vista organizada de los datos y una forma de examinar los datos desde cualquier perspectiva que desee. En este contexto, los componentes de un sistema de información se conocen como elementos de configuración (CI). Un (CI) puede ser cualquier elemento imaginable de TI, incluyendo software, hardware, documentación personal, así como cualquier combinación de ellos. Los procesos de gestión de la configuración tratan de especificar, controlar y realizar seguimiento de elementos de configuración y los cambios introducidos en ellos de manera integral y sistemática.
- **BS7799:** Estándar británico de seguridad de la información, publicado por primera vez en 1995. En 1998, fue publicada la segunda parte. La parte primera es un conjunto de buenas prácticas para la gestión de la seguridad de la información – no es certificable- y la parte segunda especifica el sistema de gestión de seguridad de la información – es certificable Asimismo la parte primera es el origen de ISO 17799 e ISO 27002 y la parte segunda de ISO 27001. – como tal el estándar, ha sido derogado ya, por la aparición de estos últimos.
- **Características de la información:** Las principales características desde enfoque de seguridad de información son: confidencialidad, disponibilidad e integridad.
- **Cheklist:** Lista de apoyo para el auditor con los puntos a auditor, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo, Este tipo de listas también se pueden utilizar durante la implantación del SGSI para facilitar su desarrollo.
- **CobiT – Control Objectives for information and related technology:** (Objetivos de Control para la información y tecnologías relacionadas): Publicados y mantenidos por ISACA, sus siglas en inglés (Information System Audit and Control association) Asociación de auditoría y control de tecnología de Información rectores, actualizados, internacionales y generalmente aceptados para ser empleados por gerentes de empresas y auditores.

- **Compromiso de la dirección:** Alineamiento firme de la dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI.
- **Cómputo forense:** El cómputo forense, también llamado informática forense, computación forense, análisis forense digital o examinación forense digital, es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.
- **Confiabilidad:** Se puede definir como la capacidad de un producto de realizar su función de la manera prevista, de otra forma, la confiabilidad se puede definir también como la probabilidad en que un producto realizará su función prevista sin incidentes por un período de tiempo especificado y bajo condiciones indicadas.
- **Confidencialidad:** Acceso a la información por parte únicamente de quienes esté autorizados, según ISO 1335-1:2004, característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.
- **Control:** Son todas aquellas políticas, procedimientos, prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.
- **Control correctivo:** Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas. Supone que la amenaza ya se ha materializado pero que se corrige.
- **Control detectivo:** Control que reduce la posibilidad de materialización de una amenaza, ejemplo por medio de avisos disuasorios.
- **Control preventivo:** control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.
- **Denegación de servicios:** Acción iniciada por agentes externos (personas, grupos, organizaciones) con el objetivo de imposibilitar el acceso a los servicios y recursos de una organización durante un período indefinido de tiempo. La mayoría de ocasiones se busca dejar fuera de servicio los servidores informáticos de una compañía o en su defecto en situaciones más complejas ocasionar graves daños, para que no puedan utilizarse ni consultarse servicios importantes. Un aspecto a resaltar es el gran daño a la imagen y reputación de las entidades que estas acciones dejan en el ambiente público.
- **Desastre:** Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse afectada de manera significativa.
- **Directiva:** según ISO 13335-1:2004: Una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

- **Disponibilidad:** según ISO 13335-1:2004: característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.
- **Evaluación de riesgos:** Según ISO guía 73:2002: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.
- **Evento: según ISO 18044:2004:** suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.
- **Evidencia objetiva:** Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos, relacionados con la confidencialidad, integridad o disponibilidad de una proceso o servicio o con la existencia e implementación de un elemento del sistema de seguridad de la información.
- **FTP:** (File transfer protocol) Es un protocolo de transferencia de archivos entre sistemas conectados a una red TCP basado en la arquitectura cliente-servidor, de manera que desde un equipo cliente nos podemos conectar a un servidor para descargar y/o subir archivos en él.
- **Gestión de claves:** Controles referidos a la gestión de claves criptográficas.
- **Gusano:** (Worm): es un programa malicioso de computador que tiene la capacidad de duplicarse a sí mismo. A diferencia del virus, no altera información, aunque casi siempre causan problemas de red debido al consumo excesivo de ancho de banda del canal de internet y su gran facilidad de mutar.
- **Impacto:** resultado de un incidente de seguridad de la información.
- **Incidente:** Según ISO 18044:2004: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Información:** La información constituye un importante activo, esencial para las actividades de una organización y, en consecuencia, necesita una protección adecuada. La información puede existir de muchas maneras, es decir puede estar impresa o escrita en papel, puede estar almacenada electrónica, ser transmitida por correo o por medios electrónicos, se la puede mostrar en videos, o exponer oralmente en conversaciones.
- **Ingeniería social:** Es la manipulación de las personas para conseguir que hagan que algo debilite la seguridad de la red o faciliten Información con clasificaciones confidencial o superior. En el campo de la seguridad informática, es un método o forma de ataque con técnicas que buscan persuadir al atacado ganando su confianza, obteniendo información privilegiada de carácter personal (contraseñas de cuentas bancarias, datos personales), igualmente apropiarse de información vital para una organización. Existen en la actualidad diversidad

de medios para llevar a cabo esta actividad, un uso común es a través de correos electrónicos o llamadas al lugar de trabajo o residencia, de ahí la importancia de tener una buena cultura digital respecto a que información suministramos.

- **IPS:** Sistema de prevención de intrusos. Es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.
- **Itil It Infraestructure Library:** Un marco de gestión de los servicios de tecnologías de la información.
- **Keyloggers:** Software o aplicaciones que almacenan información digitada mediante el teclado de un computador por un usuario; es común relacionar este término con malware del tipo Daemon (demonio), es decir, actúa como un proceso informático que no interactúa con el usuario, ya que se ejecuta en segundo plano. Usualmente puede ser un tipo de software o un dispositivo hardware que se encarga de registrar las pulsaciones que se hacen con el teclado, para posteriormente memorizarlas en un archivo o enviarlas a través de internet.
- **Legalidad:** El principio de legalidad o primacía de la ley es un principio fundamental del derecho público conforme al cual todo ejercicio del poder público debería estar sometido a la voluntad de la ley de su jurisdicción y no a la voluntad de las personas (ej. el Estado sometido a la constitución o al imperio de la ley) . Por esta razón se dice que el principio de legalidad establece la seguridad jurídica, seguridad de información, seguridad informática y garantía de la información.
- **No conformidad:** Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.
- **No conformidad grave:** Ausencia o fallo de uno o varios requerimientos de la ISO 27001 que, basada en evidencias objetivas, permita dudar seriamente de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo inaceptable.
- **No repudio:** Los activos de información deben tener la capacidad para probar que una acción o un evento han tenido lugar, de modo que tal evento o acción no pueda ser negado posteriormente.
- **Pdca - Plan Do Check Act:** Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (Implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI).
- **Phishing:** Tipo de delito encuadrado dentro del ámbito de las estafas, que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una

contraseña o información detallada sobre tarjetas de crédito u otra información bancaria), mediante una aparente comunicación oficial electrónica.

- **Plan de continuidad del negocio (BUSSINES CONTINUITY PLAN**): Plan orientado a permitir la continuación de las principales funcionales de la Entidad en el caso de un evento imprevisto que las ponga en peligro.
- **Plan de tratamiento de riesgos (RISK TREATMENT PLAN):** Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.
- **Política de seguridad y privacidad de la información:** Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información.
- **Punto único de contacto (PUC):** Entiéndase como mesa de ayuda de acuerdo a las mejores prácticas basadas en ITIL.
- **Protección a la duplicidad:** La protección de copia, también conocida como prevención de copia, es una medida técnica diseñada para prevenir la duplicación de información. La protección de copia es a menudo tema de discusión y se piensa que en ocasiones puede violar los derechos de copia de los usuarios, por ejemplo, el derecho a hacer copias de seguridad de una videocinta que el usuario ha comprado de manera legal, el instalar un software de acceso y escucharla.
- **Ransomware:** Código malicioso para secuestrar datos, una forma de explotación en el cual el atacante encripta o codifica los datos de la víctima y exige un pago por la clave de descifrado.
- **Segregación de tareas:** Separar tareas sensibles entre distintos funcionarios o contratistas para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o negligencia.
- **Seguridad de la información:** Según ISO 27002:20005: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.
- **Servicio de tratamiento de información:** Según ISO 270002:2013: cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizados para su alojamiento.
- **Spamming:** Se llama spam, correo basura o SMS basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviado en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming. La vía más usada es el correo electrónico.
- **Sniffers:** Programa de captura de las tramas de red. Generalmente se usa para gestionar la red con una finalidad docente o de control, aunque también se usa con fines maliciosos.

- **Spoofing:** falsificación de la identidad origen en una sesión la identidad es por una dirección IP o MAC Address.
- **Troyano:** Aplicación que aparenta tener un uso legítimo pero que tiene funciones ocultas diseñadas para sobrepasar los sistemas de seguridad de los equipos de cómputo.
- **Usuario:** En el presente documento se emplea para referirse a directivos, funcionarios, contratistas, terceros y otros colaboradores de la E.S.E Hospital Mental de Antioquia, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la red del HOMO y a quienes se les otorga un nombre de usuario y una clave de acceso.
- **Virus:** Programas informáticos de carácter malicioso, que buscan alterar el normal funcionamiento de una red de sistemas o computador personal, por lo general su acción es transparente al usuario y este tardo tiempo en descubrir su infección; buscan dañar, modificar o destruir archivos o datos almacenados.
- **VPN:** (Virtual Prívate Network): es una tecnología de red que permite una extensión segura de la red privada de área local (LAN) sobre una red pública o no controlada como Internet.

6. METODOLOGIA Y RECURSOS FISICOS, HUMANOS Y ECONOMICOS

La metodología adoptada para la formulación, implementación, seguimiento y mejora del Plan Institucional de Seguridad y Privacidad de la Información se fundamenta en un enfoque de gestión del riesgo y mejora continua, alineado con el ciclo PHVA (Planear – Hacer – Verificar – Actuar) establecido en la norma NTC ISO/IEC 27001 y el Modelo de Seguridad y Privacidad de la Información (MSPi).

La metodología considera el contexto institucional de la E.S.E. Hospital Mental de Antioquia – María Upegui, el tamaño y complejidad de sus procesos, la criticidad de sus activos de información y los riesgos asociados a la prestación de los servicios de salud mental.

Fases de la Metodología

A. Fase de Diagnóstico

En esta fase se realiza la identificación del estado actual de la seguridad y privacidad de la información en la Entidad, considerando, entre otros aspectos:

- Identificación y valoración de los activos de información.

- Evaluación del nivel de madurez de los controles de seguridad existentes.
- Verificación del cumplimiento de la normatividad aplicable en materia de protección de datos personales y seguridad digital.
- Identificación de brechas, vulnerabilidades y oportunidades de mejora.

B. Fase de Planificación
Con base en los resultados del diagnóstico y del análisis de riesgos, se establecen las acciones necesarias para el tratamiento de los riesgos de seguridad de la información, incluyendo:

- Identificación de las necesidades y expectativas de las partes interesadas.
- Definición de objetivos, controles y medidas de seguridad.
- Asignación de responsables y recursos.
- Elaboración y actualización de políticas, procedimientos y planes asociados al SGSI.
- Definición de indicadores de gestión y seguimiento.

C. Fase de Implementación
En esta fase se ejecutan las acciones definidas en el Plan, orientadas a la aplicación de los controles técnicos, administrativos y físicos necesarios para la protección de los activos de información, así como al fortalecimiento de la cultura organizacional en seguridad de la información.

D. Fase de Evaluación y Seguimiento
Se realiza el monitoreo y medición del desempeño del Plan y de los controles implementados, mediante:

- Seguimiento periódico al cumplimiento del cronograma de actividades.
- Revisión de indicadores de gestión.
- Ejecución de auditorías internas de seguridad de la información.
- Análisis de incidentes y eventos de seguridad.

E. Fase de Mejora Continua
Con base en los resultados de la evaluación, se definen e implementan acciones correctivas y de mejora que permitan fortalecer de manera progresiva el Sistema de Gestión de Seguridad de la Información, asegurar su sostenibilidad y mantener su alineación con los cambios normativos, tecnológicos y organizacionales.

RECURSOS HUMANOS

La gestión de la seguridad y privacidad de la información requiere personal con competencias técnicas, administrativas y operativas, así como con conocimiento del contexto institucional y del marco normativo aplicable. En este sentido, la Entidad contará con los siguientes roles y perfiles, sin perjuicio de las responsabilidades que

recaen sobre todos los funcionarios, contratistas y terceros como custodios de la información:

Responsable de la Seguridad y Privacidad de la Información (CISO o rol equivalente): Encargado de coordinar, orientar y supervisar la implementación del Modelo de Seguridad y Privacidad de la Información (MSPi), así como de articular las actividades del SGSI con el Sistema Integrado de Gestión y la planeación institucional.

Profesionales del área de Tecnologías de la Información y las Comunicaciones (TIC): Ingenieros y técnicos responsables de la administración de la infraestructura tecnológica, los sistemas de información, las redes de comunicaciones, los centros de datos y los servicios asociados, quienes apoyan la implementación de los controles técnicos y operativos definidos en el Plan.

Personal de apoyo técnico y operativo: Técnicos y tecnólogos encargados de la ejecución de actividades de soporte, mantenimiento preventivo y correctivo, atención a usuarios y operación diaria de los servicios tecnológicos, conforme a los procedimientos establecidos.

Funcionarios, contratistas, proveedores y terceros: Todos los usuarios de la información y de los recursos tecnológicos de la Entidad, quienes tienen la obligación de cumplir las políticas, lineamientos y controles definidos en el presente Plan, así como de participar en las actividades de capacitación y sensibilización en seguridad de la información.

La asignación de funciones, responsabilidades y niveles de autoridad será definida y formalizada mediante los actos administrativos, manuales de funciones, contratos y demás instrumentos institucionales aplicables, garantizando el principio de responsabilidad probada.

Recursos Financieros

La E.S.E. Hospital Mental de Antioquia – María Upegui dispondrá de los recursos financieros necesarios para la ejecución del Plan Institucional de Seguridad y Privacidad de la Información, de acuerdo con las prioridades definidas en el análisis de riesgos, el Plan de Acción institucional y la disponibilidad presupuestal.

Los recursos financieros estarán orientados, entre otros aspectos, a:

- La adquisición, renovación y mantenimiento de infraestructura tecnológica y de seguridad.

- La implementación de herramientas y soluciones de seguridad de la información.
- La contratación de servicios especializados, cuando se requiera.
- La ejecución de programas de capacitación y sensibilización.
- El desarrollo y actualización de planes de contingencia, continuidad y recuperación.

La gestión de los recursos financieros se realizará conforme a los principios de eficiencia, eficacia, economía y transparencia, y estará sujeta a los mecanismos de planeación, seguimiento y control establecidos por la Entidad.

7. ACTIVIDADES (CRONOGRAMA)

ACTIVIDAD N°	ACTIVIDADES/ ACCIONES A DESARROLLAR	PRODUCTO O EVIDENCIA	AREA RESPONSABLE	FECHA DE ENTREGA											
				Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
1.	Definir y/o actualizar el marco institucional de seguridad y privacidad de la información, políticas y lineamientos, en el marco del MSPi y apoyado en el SGSI.	Políticas y lineamientos aprobados, actas de comité, matrices de control.	Profesional universitario Gestión de las Tic's			x									
2.	Ejecutar el plan de implementación y mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPi).	Informes de avance, matrices de seguimiento, actas del comité de seguridad y privacidad de la información	Profesional universitario Gestión de las Tic's		x		x		x		x		x		x
3.	Realizar seguimiento y evaluación del desempeño de la seguridad y	Indicadores de gestión, reportes de seguimiento,	Profesional universitario Gestión de las Tic's			X			X			X			X

	privacidad de la información.	planes de mejora.													
4.	Realizar el análisis y tratamiento de riesgos de seguridad de la información conforme a MSPi e ISO 27005.	Matriz de riesgos, plan de tratamiento.	Profesional universitario Gestión de las Tic's						X						
5.	Actualizar y mantener el Modelo de Seguridad y Privacidad de la Información (MSPi) institucional.	Documento MSPi actualizado y aprobado.	Profesional universitario Gestión de las Tic's				X								
6.	Documentar y/o actualizar el plan de contingencia y el procedimiento de gestión de incidentes de seguridad de la información.	Planes documentados, registros de incidentes, actas de revisión.	Profesional universitario Gestión de las Tic's				x					x			
7.	Definir, actualizar y evaluar los planes de continuidad del negocio y recuperación ante desastres.	BIA, planes de continuidad, resultados de pruebas o simulacros.	Profesional universitario Gestión de las Tic's						X						X
8.	Gestionar la adquisición e implementación de herramientas tecnológicas para fortalecer la seguridad de la información, según el análisis de riesgos.	Contratos, licencias, informes de implementación.	Profesional universitario Gestión de las Tic's					X					X		
9.	Realizar análisis de vulnerabilidades y, cuando aplique, pruebas de seguridad sobre los sistemas de información.	Informes técnicos, planes de remediación.	Profesional universitario Gestión de las Tic's								x				
10.	Diseñar y ejecutar el programa de capacitación, sensibilización y reinducción en seguridad y privacidad de la información.	Cronograma de capacitación, listas de asistencia, material de apoyo.	Profesional universitario Gestión de las Tic's			X			X			X			X

8. DIFUSIÓN

Mecanismo de elaboración	La metodología utilizada para la realización fue basada con la normatividad vigente, adaptándola a la E.S.E. Hospital Mental de Antioquia María Upegui – HOMO.
Mecanismo de difusión	El Plan será dado a conocer a los líderes involucrados, estos a su a vez lo darán a conocer a sus colaboradores; posteriormente se montará en la página web institucional para la consulta del público en general.
Mecanismos de capacitación	Se socializará de forma verbal por parte del líder o responsable de ejecución del plan con su equipo de trabajo y las partes interesadas.
Mecanismos de evaluación	Será evaluado y monitoreado por medio de un seguimiento según el cronograma de ejecución de cada actividad, y será la oficina de Planeación quien lo realice.
Mecanismos de retroalimentación	Se hará un acompañamiento constante a las áreas que intervengan en cada plan, para que las mismas entreguen oportunamente y con claridad el desarrollo de las actividades programadas.

9. SEGUIMIENTO

Desde el área de planeación se realiza seguimiento de forma mensual y se lleva indicador de resultado de forma trimestral en el comité de gestión y desempeño.

Indicador de seguimiento: Proporción de ejecución del Plan de seguridad y privacidad de la información

Número de actividades ejecutadas en el período / Número de actividades programadas en el plan durante el periodo

RANGO		
0 – 60%	Rojo	Baja
61 – 89%	Amarillo	Media
90 – 100%	Verde	Alta

10. NOMBRES DE RESPONSABLE DE DILIGENCIAMIENTO Y EJECUCIÓN DEL PLAN

Nombre	Cargo
Carlos Andrés Muñoz Velez	Ingeniero de Sistemas (TI)
Mauricio Pulgarín	Profesional universitario encargado de gestión de las Tic's
Henry Restrepo Molina	Técnico
Edwin Agudelo	Técnico

Edwin Agudelo	Técnico

11. CONTROL DE CAMBIOS

ELABORÓ	Mauricio Pulgarin – Ingeniero de telecomunicaciones
ACTUALIZÓ	Mauricio Pulgarin – Ingeniero de telecomunicaciones
APROBÓ	Comité de Gestión y Desempeño
VERSIÓN	03
MOTIVO DE ACTUALIZACIÓN	Actualización del Plan Institucional de Seguridad y Privacidad de la Información con el fin de alinearlo al Modelo de Seguridad y Privacidad de la Información (MSPi) del Ministerio de Tecnologías de la Información y las Comunicaciones, fortalecer la gestión del riesgo de seguridad digital, ajustar el cronograma de actividades y mejorar los mecanismos de seguimiento, control y responsabilidad probada para la vigencia correspondiente.
FECHA DE ACTUALIZACIÓN	15/01/2026