Hospital Departamental
Psiquiátrico Universitario
Del Valle E.S.E.

CÓDIGO	PLA-GIN-04
VERSIÓN	01
VIGENCIA	ENERO DE 2026

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION VIGENCIA 2026

PLA-GIN-04

INTRODUCCIÓN

El Hospital Departamental Psiquiátrico Universitario del Valle E.S.E ha venido gestionando e implementando acciones en toda la entidad con el objetivo de fortalecer las capacidades institucionales en todos sus procesos para dar cumplimiento a las disposiciones legales vigentes en materia de seguridad y privacidad de la información.

La alta dirección del Hospital Departamental Psiquiátrico Universitario del Valle E.S.E en respuesta a los requerimientos emanados de las recomendaciones de las auditorías externas, auditorías internas y requerimientos de MinTIC, entiende la Seguridad y la privacidad de la Información como un elemento habilitador transversal al gobierno de las tecnologías de la información y la seguridad de la información en el Hospital y asume esta práctica por medio de la implementación de los controles que define la norma NTC ISO 27001 en su última versión y la implementación del Sistema de Gestión de Seguridad de la Información – SGSI.

Con la aplicación de estos controles de seguridad en todos los activos de la infraestructura tecnológica del Hospital y en todos sus procesos, trámites, servicios, y sistemas de información, se logra que este plan de seguridad y privacidad de la información se alinee con los objetivos estratégicos del Hospital Departamental Psiquiátrico Universitario del Valle E.S.E.

La implementación de este plan ayudará a identificar las responsabilidades en materia de seguridad y privacidad de la información, así como el desarrollo de las actividades necesarias para la identificación y clasificación de los activos de información con el fin de aplicar los controles de confidencialidad, integridad y disponibilidad bajo un entorno de mejora continua dentro del ciclo PHVA.

Los procesos involucrados en cada grupo son:

PRIMER GRUPO	SEGUNDO GRUPO
• Direccionamiento estratégico • Sistema Integrado de Gestión • Sistema de Información y Atención al Usuario • Urgencias • Consulta Externa • Hospitalización • Intervención Social y Comunitaria • Docencia – Servicio e Investigación • Gestión de la Información	• Mercadeo y Comunicaciones • Gestión Financiera • Gestión Logística • Gestión de Ambiente Físico • Gestión de Talento Humano

Tabla 1 Grupos de implementación del MSPI

1. OBJETIVO

Establecer un marco de acción orientado al fortalecimiento del SGSI-Sistema de Gestión de Seguridad de la Información, sobre los activos contenedores de información en todos los procesos del Hospital y al mismo tiempo definir las acciones, tendientes a fortalecer los esquemas de la seguridad y privacidad de la información de la entidad, acciones que deben ser gestionadas por todos los funcionarios y/o contratistas, mediante la implementación de la Política de Seguridad y Privacidad de la información, y la política de tratamiento de datos personales, así de esta forma fortalecer la confianza de los grupos de valor y de interés en el Hospital.

2. ALCANCE

El Hospital Departamental Psiquiátrico Universitario del Valle E.S.E. ha adoptado el Modelo de Seguridad y Privacidad de la Información -MSPI propuesto por MINTIC y basado en la norma ISO 27001:2022, mediante la ejecución de planes de trabajo independientes para los temas de seguridad y de privacidad de la información, por lo cual se segmentan las dependencias de la Entidad para la aplicación de los cronogramas de trabajo.

3. CONDICIONES GENERALES

No aplican condiciones generales al plan

4. 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 acceso 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 esta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27001).

Activos de Información y recursos: se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa del Hospital, órgano u organismo. (CONPES 3854 de 20116).

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo. (ISO/IEC 27000).

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

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: Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

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

Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

Datos Personales Privados: Es el dato que por su naturaleza intima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)

Datos Personales Mixtos: Para efectos de este documento es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos Personales Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

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

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).

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), 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.

MIPG: Modelo Integrado de Planeación y Gestión.

MSPI: Modelo de Seguridad y Privacidad de la Información.

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

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).

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)

Responsabilidad Demostrada: Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

Responsable del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art. 3).

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 en cualquier medio: impreso o digital. (ISO/IEC 27000).

Seguridad digital: Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.

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).

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

Partes interesadas (Stakeholder): Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

Confidencialidad: Propiedad de la información que la hace no disponible o que no sea divulgada a individuos, entidades o procesos no autorizados.

Integridad: Propiedad de la información que busca preservar su exactitud y completitud.

Disponibilidad: Propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.

Sistema de Gestión de Seguridad de la Información: Es el conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan dentro del Hospital.

Controles: Medida que permite reducir o mitigar un riesgo.

5. MARCO LEGAL

Constitución Política de Colombia. Artículos 15, 209 y 269.
Ley 527 de 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del Habeas 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.
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.
Ley 1437 de 2011, Capítulo IV. "Utilización de medios electrónicos en el procedimiento administrativo". "Los procedimientos y trámites administrativos podrán realizarse a través de medios electrónicos. Para garantizar la igualdad de acceso a la

administración, la autoridad deberá asegurar mecanismos suficientes y adecuados de acceso gratuito a los medios electrónicos, o permitir el uso alternativo de otros procedimientos.

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

Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.

Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.

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 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

Decreto 1074 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.

Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Decreto 1080 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Cultura.

Decreto 1081 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.

Decreto 1083 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública", el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de "11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital".

CONPES 3854 de 2016. Política Nacional de Seguridad digital.

Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.

Decreto 612 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. Artículos 1 y 2 relacionados con el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y el Plan de Seguridad y Privacidad de la Información.

Decreto 1008 de 2018. Por medio del cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

CONPES 3975 de 2019. Política nacional para la transformación digital e inteligencia artificial.

Ley 1955 de 2019. Por el cual se expide el Plan Nacional de Desarrollo 2018-2022. "Pacto por Colombia, Pacto por la Equidad". Artículo 147. Transformación Digital Pública. Las entidades estatales del orden nacional deberán incorporar en sus respectivos planes de acción el componente de transformación digital siguiendo los estándares que para este propósito defina el Ministerio de Tecnologías de la Información y las Comunicaciones. Artículo 148. Gobierno Digital como Política de Gestión y Desempeño Institucional. Todas las entidades de la administración pública deberán adelantar las acciones que señale el Gobierno nacional a través del Ministerio de Tecnologías de la Información y las Comunicaciones para la implementación de la política de Gobierno Digital.

CONPES 3995 DE 2019. Política nacional de confianza y seguridad digital.

Decreto 2106 de 2019. Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública

6. DESCRIPCION

DESARROLLO DEL PLAN

El Hospital Departamental Psiquiátrico Universitario del Valle E.S.E., ha adoptado la Política de Seguridad de la Información, como parte del sistema integral de gestión, y para lograr su implementación y adopción ha creado un plan estratégico de seguridad de la información, con el objetivo de avanzar en la implementación orientado a dar cumplimiento a las directrices de Min tic - Ministerio de Tecnologías de Información y de las Comunicaciones, en cuanto a la adopción e implementación del Modelo de Seguridad y Privacidad de la Información.

Todas las acciones que se proponen en este plan están orientadas al fortalecimiento de la Política de Seguridad Digital como habilitador de dicha política. Así mismo, en atención tanto a lo especificado en el modelo de seguridad y privacidad, como lo estipulado en el estándar NTC ISO 27001:2022, se aborda la identificación, valoración, tratamiento y gestión de riesgos de seguridad digital, y la ciberseguridad como parte fundamental del modelo.

A continuación, se presentan las fases de implementación del Modelo de Seguridad y Privacidad de la información para El Hospital Departamental Psiquiátrico Universitario del Valle E.S.E.

Ciclo del Modelo de Seguridad y Privacidad de la Información
Fuente: Anexo 1 Modelo de Seguridad y Privacidad de la información

Detalle de actividades del plan de trabajo según alcance y vigencia

FASE	ACTIVIDAD	TAREA POR DESARROLLAR PARA EL PLAN	FECHA FINALIZACIÓN	RESPONSABLE DEL CUMPLIMIENTO Y SEGUIMIENTO
P	Diagnóstico con herramienta MSPI del MINTIC	Realizar la actualización del instrumento de autodiagnóstico vigencia 2025	Febrero 2026	Profesional Universitario de la Oficina de Sistemas
P	Generar los Planes de Gestión de la Seguridad y Privacidad	Generar los Planes que sostendrán la Implementación de la Seguridad, Ciberseguridad y Privacidad de la Información: * Diseño y documentación y envío de aprobación del plan de seguridad y privacidad de la información * Diseño y documentación y envío de aprobación del plan integral de privacidad (protección de datos personales) * Diseño y documentación y envío a aprobación del plan de capacitación y concientización de la seguridad y privacidad	Enero a diciembre 2026	Profesional Universitario de la Oficina de Sistemas
H	Gestión y Gobierno de la Seguridad y Ciberseguridad de la información	* Adopción e implantación de un SGSI * Fortalecer y gestionar la Implementación del sistema de gestión de riesgos de la entidad. * Revisar fortalecer y actualizar las políticas de Seguridad, ciberseguridad y privacidad de la información del Hospital. * Se deben identificar basados en la guía de Mintic la infraestructura crítica del Hospital y definir los activos y procesos de seguridad * Definir y documentar los niveles de autorización de accesos a los sistemas de información. * Revisión y actualización de los procedimientos de Seguridad y privacidad de la información (MINIMO 15 PROCEDIMIENTOS BASE DEL SGSI) entre los cuales deben estar mínimo: * Procedimiento de gestión de contraseñas * Procedimiento de creación y gestión de usuarios * Procedimiento de Recibo, retiro y devolución de activos de información. * Procedimiento de gestión de Incidentes. * Procedimiento de Tratamiento de riesgos. * Procedimiento de Acceso seguro a los sistemas de información * Procedimiento de gestión de códigos y software malicioso * Procedimiento de Respaldo y recuperación de la	Enero a diciembre 2026	Profesional Universitario de la Oficina de Sistemas

		información * Procedimiento de borrado seguro de la Información.		
H	Gestión delegada de Sistema de Gestión de Ciberseguridad	* Administración y Monitoreo de la consola de antivirus y equipo de seguridad perimetral (Sophos) * Administración y Monitoreo de la consola de equipo de seguridad perimetral (Sophos) * Administración y Monitoreo de los indicadores de seguridad * Administración y Monitoreo de los recursos TIC con la centralización y almacenamiento de logs para equipos de telemática (Switches, Routers, Accesspoints), en la herramienta Zabbix	Enero a diciembre 2026	Profesional Universitario de la Oficina de Sistemas
H	Implementación de la Seguridad y Ciberseguridad de la información y Gestión de Vulnerabilidades.	* Implementar el plan de seguridad y privacidad de la información * Implementar mínimo 18 de los controles de requisito de la Norma ISO 27001:2022. * Implementar mínimo 50 de los controles de seguridad del ANEXO A de la norma ISO 27001:2022. * Implementar controles en el equipo de seguridad perimetral y en la red, tales como reglas de filtrado web en los firewalls, sistemas de detección y prevención de intrusiones (IDS/IPS) y segmentación de redes, para proteger la infraestructura. * Fortalecer la gestión de accesos a los sistemas de información del Hospital, estableciendo mecanismos robustos de autenticación, autorización y auditoría en sistemas críticos. * Desplegar soluciones de cifrado de datos tanto en tránsito como en reposo, para salvar la información sensible y garantizar la confidencialidad. * Realizar un diagnóstico exhaustivo de las vulnerabilidades de la infraestructura TI del Hospital, evaluando la configuración de redes, servidores, end points y dispositivos, para identificar potenciales fallas de seguridad y riesgos existentes.	Enero a diciembre 2026	Profesional Universitario de la Oficina de Sistemas

H	Mantenimiento del MSPI	* Evaluación del cumplimiento del MSPI de acuerdo con lo exigido por MINTIC. * Fortalecimiento de la implementación del MSPI * valoración y evaluación del cumplimiento del MSPI * Elaboración del plan de acción para la mejora continua del MSPI, se debe entregar un informe final del estado actual de cumplimento del MSPI de acuerdo con el requerimiento de MINTIC.	Enero 2026 a diciembre 2026	Profesional Universitario de la Oficina de Sistemas
H	Gestión efectiva de incidentes de seguridad de la información	* Desarrollar y poner en marcha un plan de respuesta a incidentes que incluya protocolos para la contención, mitigación, análisis forense y comunicación ante eventos de ciberseguridad por medio del diseño y documentación de un procedimiento el cual deben dejar documentado y en proceso de aprobación de la alta gerencia. * Establecer un sistema de reporte y seguimiento de incidentes que asegure la comunicación oportuna con la alta dirección y permita la trazabilidad de las acciones correctivas. * Incluir en los procesos de gestión de incidentes la valoración de los eventos de seguridad y generar toma de decisiones. * Crear un plan de respuesta ante incidentes el cual debe quedar documentado y entregado para aprobación por parte de la alta dirección (mintic) * Generar en el proceso acciones para aprendizaje de los eventos de incidentes. * Realizar pruebas técnicas de los sistemas de contingencias para validar la continuidad de los servicios y procesos críticos de la entidad en no menos de 4 servicios críticos y dejar informe documentado de los resultados y una sección de recomendaciones para la mejora continua.	Enero a diciembre 2026	Profesional Universitario de la Oficina de Sistemas

V	Gestión de Auditorias de Seguridad y Ciberseguridad y de la mejora continua	* Elaborar ejercicios de valoración y evaluación del cumplimiento de los controles de seguridad y privacidad de la información * Realizar auditorías y pruebas de penetración tipo pentesting o ethical hacking de forma periódica durante la vigencia del contrato mínimo 2 veces a cada activo, evaluando la efectividad de los controles implementados, como mínimo a 5 servidores locales de la entidad, 2 equipos de usuarios y 3 aplicaciones web como activos críticos de la entidad. * Realizar auditorías a la gestión del riesgo tecnológico debe entregar las matrices de riesgos finales posterior a la identificación y valoración para aprobación de la alta gerencia. * Diseñar planes de acción y de mejora continua para correcta implementación de los controles alineados a la ISO 27001. * Gestionar las vulnerabilidades identificadas y mejoramiento de seguridad de los informes de vulnerabilidades y hacking ético-realizados en la institución, a través de la implementación de un plan de mitigación de brechas de seguridad. * En el proceso de mejora continua debe adoptar y ejecutar las recomendaciones de la auditoria del proveedor anterior * Realizar procesos de parcheo a todos los sistemas operativos y a los aplicativos de los sistemas de información como mínimo 12 servidores de la infraestructura local.	Enero a diciembre 2026	Profesional Universitario de la Oficina de Sistemas
A	Gestionar la mejora continua	Ejecutar los planes de mejora para sanetizar los pendientes de las revisiones técnicas y ejecutar los planes de acción emanados de las auditorias de Control Interno.	Diciembre 2026	Profesional Universitario de la Oficina de Sistemas

Tabla 2 cronograma plan de trabajo según alcance y vigencia

Metas

Para la vigencia 2026 se plantearon las siguientes metas

- Realizar el levantamiento de activos de información del Hospital Departamental Psiquiátrico Universitario del Valle E.S.E. en todos los procesos.
- Realizar el 100% de la identificación, valoración, clasificación de los riesgos de seguridad y privacidad de la información al 31 de diciembre de 2026.

- Desarrollar el 100 % de la estrategia de comunicación de las políticas de seguridad y privacidad de la información, para darlas a conocer a los servidores públicos de la entidad.

Indicadores

Para la monitorización del presente plan se plantean los siguientes indicadores:

Indicadores	Variables	Formula
Cumplimiento del plan de seguridad y privacidad de la información	Número de actividades planeadas y ejecutadas	Número de actividades ejecutadas / Número de actividades planeadas * 100
Cumplimiento en la valoración y tratamiento de riesgos de riesgos	Numero de riesgos mitigados del plan de tratamiento	Numero de riesgos mitigados / Número de riesgos identificados * 100
Gestión efectiva de Incidentes de Seguridad	Número de incidentes de seguridad reportados	Número de Incidentes de seguridad de gestionados y cerrados / Número de Incidentes de Seguridad Reportados * 100

Periodo de implementación

El plan de seguridad se encuentra definido para la vigencia 2026, el cual contempla una revisión anual que puede implicar una posible reformulación de acuerdo con las nuevas directrices, normatividades distritales y nacionales y el resultado de seguimientos y auditorías internas. Inicialmente la ejecución del plan y el cumplimiento de las actividades se establecen para el año 2026.

7. ANEXOS

N.A

Elaborado por:	Revisado por:	Aprobado por:
ORIGINAL FIRMADO	***ORIGINAL FIRMADO***	***ORIGINAL FIRMADO***
Leydi Marcela Martínez Turriago Profesional Universitario Sistemas	**Berenice Rivera Trujillo** Líder ISC	**Stella Tafur Guerreo** Subgerente Administrativa y Financiera
Fecha: 14 de enero de 2026	**Fecha:** 16 de enero de 2026	**Fecha:** 19 de enero de 2026

VERSIÓN	DESCRIPCIÓN DEL CAMBIO	FECHA DE VIGENCIA
01	Creación del documento	Enero de 2026