

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN



ALCALDÍA DE
BUCARAMANGA

ISABU
e.s.e | INSTITUTO DE SALUD
DE BUCARAMANGA



Proceso: Gestión Tics

Subproceso: Seguridad de la información

Código: SEG- PL - 006

Versión: 04

Fecha de aprobación: 29/01/2026



	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		FECHA ELABORACIÓN: 27/01/2023
	CÓDIGO: SEG-PL-006		FECHA ACTUALIZACIÓN: 29/01/2026
	VERSIÓN: 4		PÁGINA: 1-7
			REVISÓ Y APROBÓ: Comité CIGD No.1 de 2026.

TABLA DE CONTENIDO

1.	OBJETIVO:	2
2.	ALCANCE:	2
3.	RESPONSABLE:	2
4.	DEFINICIONES	2
5.	DESARROLLO	3
5.1	AUTODIAGNÓSTICO	3
5.2	SITUACIÓN ACTUAL	3
5.3	MAPA DE RUTA	4
5.4	PLAN PARA LA IMPLEMENTACIÓN DEL MODELO DE PRIVACIDAD DE LA INFORMACIÓN Y SEGUIMIENTO A LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCION DE LA PRIVACIDAD - VIGENCIA 2025.	5
5.5	INDICADOR Y META	5
5.6	ANEXOS	5
6.	DOCUMENTOS REFERENCIADOS	6
7.	CONTROL DE MODIFICACIONES	6

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		FECHA ELABORACIÓN: 27/01/2023
	CÓDIGO: SEG-PL-006		FECHA ACTUALIZACIÓN: 29/01/2026
	VERSIÓN: 4		PÁGINA: 2-7
			REVISÓ Y APROBÓ: Comité CIGD No.1 de 2026.

1. OBJETIVO:

Establecer documento que permita determinar las actividades y lineamientos de buenas prácticas para proteger los activos de información de la institución, mediante el seguimiento de la política de Seguridad de la información, ciberseguridad y protección de la privacidad de la ESE ISABU, con el fin de asegurar el cumplimiento de la integridad, disponibilidad, y confidencialidad de los activos de la información.

2. ALCANCE:

El plan de seguridad y privacidad de la información, inicia en fortalecer y definir acciones para el seguimiento de la política de Seguridad de la información, ciberseguridad y protección de la privacidad, determinada desde el Proceso de Gestión de las Tic's, para el conocimiento y cumplimiento de la misma mediante los procesos estratégicos y misionales de la ESE ISABU y concluye con la ejecución de acciones que realizará la institución para el cumplimiento y seguimiento a la política en la vigencia actual.

3. RESPONSABLE:

Profesional especializado de sistemas,
Profesional especializado en seguridad informática
Profesional especializado en infraestructura
Profesional apoyo sistemas de información.


4. DEFINICIONES

Activo: Un activo es un bien que la empresa posee y que puede convertirse en dinero u otros medios líquidos equivalentes. (debitoor, s.f.)

Amenazas: Robo de información, Destrucción de información, Anulación del funcionamiento de los sistemas, Suplantación de la identidad, publicidad de datos personales o confidenciales, cambio de información, Robo de dinero o estafas. (Vegagestion, S.F.)

Confidencial: Significa que la información no esté disponible o revelada a individuos, entidades o procesos no autorizados.
Correo Electrónico Institucional: Es el servicio basado en el intercambio de información a través de la red y el cual es provisto por la ESE ISABU, para los funcionarios, contratistas y practicantes autorizados para su acceso. El propósito principal es compartir información de forma rápida, sencilla y segura. El sistema de correo electrónico puede ser utilizado para el intercambio de información, administración de libreta de direcciones, manejo de contactos, administración de agenda y el envío y recepción de documentos, relacionados con las responsabilidades institucionales.

Custodia de la información: Es el encargado de la administración de seguridad de información. Dentro de sus responsabilidades se encuentra la gestión del Plan de Seguridad de Información, así como la coordinación de esfuerzos entre el personal de sistemas y los responsables de las otras áreas de la Entidad, siendo estos últimos los responsables de la información que utilizan. Asimismo, es el responsable de promover la seguridad de información en todo el Instituto con el fin de incluirla en el planteamiento y ejecución de los objetivos institucionales.

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		FECHA ELABORACIÓN: 27/01/2023
	CÓDIGO: SEG-PL-006		FECHA ACTUALIZACIÓN: 29/01/2026
	VERSION: 4		PÁGINA: 3-7
			REVISÓ Y APROBÓ: Comité CIGD No.1 de 2026.

Disponibilidad de la información: La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. A groso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

Gestión de activos de información: es una tarea de las gerencias de seguridad o de gestión de la información que involucra el diseño, establecimiento e implementación de un proceso que permita la identificación, valoración, clasificación y tratamiento de los activos de información más importantes del negocio. Un activo de información en el contexto de la norma ISO/IEC 27001 es: “algo que una organización valora y por lo tanto debe proteger”. (Varela, s.f.)

Integridad: La integridad de datos es un término usado para referirse a la exactitud y fiabilidad de los datos. Los datos deben estar completos, sin variaciones o compromisos del original, que se considera confiable y exacto. (Información, s.f.)

Vulnerabilidades: Una vulnerabilidad es un fallo o debilidad de un sistema de información que pone en riesgo la seguridad de la misma. Se trata de un “agujero” que puede ser producido por un error de configuración, una carencia de procedimientos o un fallo de diseño. (ambit, s.f.)

5. DESARROLLO

5.1 AUTODIAGNÓSTICO


Durante los periodos 2023, 2024 y 2025 se ha logrado el cumplimiento del 100% de las actividades previstas en el marco del Plan de Seguridad y Privacidad de la Información de la E.S.E. ISABU. Estas acciones incluyeron la elaboración, publicación y actualización anual del plan, la sensibilización institucional sobre políticas de seguridad de la información y protección de datos personales, así como la ejecución de medidas técnicas y procedimentales orientadas a la seguridad digital.

Entre las actividades más relevantes se destacan la realización de pruebas de phishing, la actualización de licenciamientos de seguridad, la implementación de controles tecnológicos y procedimentales, y la documentación de informes de análisis y seguimiento. Estas medidas han permitido fortalecer la postura de seguridad digital de la entidad, garantizando la integridad, disponibilidad y confidencialidad de la información, en cumplimiento de los estándares normativos nacionales e internacionales.

La ejecución exitosa de los planes en los tres años evidencia un proceso de maduración progresiva, pasando de un enfoque inicial en seguridad digital hacia la integración de la ciberseguridad y la privacidad de la información, con indicadores de gestión y roles especializados. Este avance contribuye al fortalecimiento de la cultura institucional en seguridad, al aseguramiento de los activos tecnológicos y a la preparación frente a riesgos emergentes del entorno digital.

5.2 SITUACIÓN ACTUAL

La E.S.E ISABU ha realizado actividades orientadas a la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI), Para lo cual se tiene aprobada la política de seguridad de la información ciberseguridad y protección de la privacidad. Siendo conscientes que la información es uno de los activos más importantes para la Institución. En cumplimiento a las políticas, establece El Plan De Seguridad Y Privacidad De La Información.

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		FECHA ELABORACIÓN: 27/01/2023
	CÓDIGO: SEG-PL-006		FECHA ACTUALIZACIÓN: 29/01/2026
	VERSIÓN: 4		PÁGINA: 4-7
			REVISÓ Y APROBÓ: Comité CIGD No.1 de 2026.

El cual contribuye a que la E.S.E ISABU, por medio de su implementación incrementa los niveles de confidencialidad, integridad y disponibilidad de la información, fomentando una cultura institucional, en cuanto a la necesidad de preservar los activos de información Cumpliendo con las políticas y normativas institucionales, así como lo definido en la estrategia de Gobierno Digital y la Política Nacional de Seguridad Digital. Todo esto con el fin de minimizar los riesgos y el impacto de algún evento que atente contra la información que se maneja en los diversos procesos de la entidad. Aún más teniendo en cuenta la labor tan importante que desempeña el E.S.E ISABU y todas las normas que actualmente se tienen sobre seguridad de la información y protección de datos.

Teniendo en cuenta que el costo para recuperar la información y restituir el sistema, siempre será mayor al costo de la aplicación de mecanismos y análisis para evitar estos posibles eventos y cumplir con las normativas establecidas. Todas los mecanismos o las medidas de seguridad se llevarán a cabo con el fin de contar con información de calidad. Preservando los principios de la seguridad de la información:

- Integridad.
- Disponibilidad.
- Confidencialidad.

Así mismo, en atención tanto a lo especificado en la política de seguridad de la información, ciberseguridad y protección de la privacidad, como lo estipulado en el estándar NTC ISO 27001:2022, se aborda la identificación, valoración, tratamiento y gestión de riesgos de seguridad informática frente a ciberamenazas, como aporte fundamental a las acciones que se deben desarrollar en el marco del modelo de seguridad y Privacidad de la Información de la entidad.

La ESE ISABU desde el 2020 realiza seguimiento al Plan de seguridad y privacidad de la Información, evidenciado mediante actividades ejecutadas de forma anual reportadas mediante el Plan de acción y planes estratégicos. A continuación, se relaciona el Mapa de Ruta creado para la vigencia 2025

5.3 MAPA DE RUTA

Para la construcción del plan de seguridad y privacidad de la información se realizará con la metodología del ciclo PHVA para la vigencia actual de las actividades generadas en el plan de acción.

PLANEACION


Diseñar estrategias, políticas y planes para garantizar la seguridad y privacidad de la información, teniendo en cuenta la identificación de los riesgos y amenazas, definir controles y procedimientos, asignación de recursos.

HACER

Implementar las medidas, políticas y procedimientos establecidos teniendo en cuenta los controles de seguridad, capacitación de personal, mecanismos de monitoreo, simulacros y pruebas que permitan la mitigación de los riesgos de seguridad de la información

VERIFICAR

Evaluar y medir el desempeño de las actividades de seguridad y privacidad de la información.

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		FECHA ELABORACIÓN: 27/01/2023
	CÓDIGO: SEG-PL-006		FECHA ACTUALIZACIÓN: 29/01/2026
	VERSION: 4		PÁGINA: 5-7
			REVISÓ Y APROBÓ: Comité CIGD No.1 de 2026.

ACTUAR

Implementar mejoras y correcciones para optimizar la seguridad y privacidad de la información.

5.4 PLAN PARA LA IMPLEMENTACIÓN DEL MODELO DE PRIVACIDAD DE LA INFORMACIÓN Y SEGUIMIENTO A LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCION DE LA PRIVACIDAD - VIGENCIA 2026

Teniendo en cuenta las políticas seguridad de la información, ciberseguridad y protección de la privacidad aprobada por la ESE ISABU, a continuación, se establece el Plan de seguridad y privacidad de la información.

Tabla 1 Actividades Plan de de seguridad y privacidad de la información

No.	Ciclo PHVA	Meta	ACTIVIDAD	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE
1	Planear	1	Actualizar el plan de seguridad y privacidad de la información para la vigencia 2026	Actualizar el plan de seguridad y privacidad de la información para la vigencia 2026	Profesional especializado de sistemas/ Profesional especializado en seguridad de la información
2	Hacer	1	Elaborar cronograma de las actividades del plan de seguridad y privacidad de la información para la vigencia 2026	Elaborar cronograma de las actividades del plan de seguridad y privacidad de la información para la vigencia 2026	Profesional especializado de sistemas/ Profesional especializado en seguridad de la información
3	Hacer	1	Publicar en página web el Plan de seguridad y privacidad de la información para la vigencia 2026	Link de publicación en página web	Gestión de las TIC
4	Hacer	1	Socializar el plan de seguridad y privacidad de la información a través de correo electrónico con los líderes de procesos y su cronograma 2026	Correo electrónico de la socialización del plan de seguridad y privacidad de la información	Profesional especializado de sistemas/ Profesional especializado en seguridad de la información
5	Hacer	4	Ejecutar las actividades del plan de seguridad y privacidad de acuerdo cronograma de la vigencia 2026	Excel de la ejecución trimestral de las actividades del plan de seguridad y privacidad de la información	
6	Verificar	100%	Medir y analizar trimestralmente el cumplimiento de la ejecución del cronograma del Plan de seguridad y privacidad de la información para la vigencia 2026	Medir y analizar trimestralmente el cumplimiento de la ejecución del cronograma del Plan de seguridad y privacidad de la información para la vigencia 2026	Profesional especializado de sistemas/ Profesional especializado en seguridad de la información
7	Actuar	1	Actuar frente a las desviaciones encontradas en el plan de seguridad y privacidad de la información para la vigencia 2026	Actuar frente a las desviaciones encontradas en el plan de seguridad y privacidad de la información para la vigencia 2026	Profesional especializado de sistemas/ Profesional especializado en seguridad de la información

Fuente: Oficina de Gestión de las TIC's


5.5 INDICADOR Y META

Gestión de Ejecución del Plan de seguridad y privacidad de la información

porcentaje de cumplimiento del plan de acción anual del de seguridad y privacidad de la información (No. de acciones ejecutadas / No. de acciones programadas) *100

Meta: 100%

5.6 ANEXOS

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		FECHA ELABORACIÓN: 27/01/2023
	CÓDIGO: SEG-PL-006		FECHA ACTUALIZACIÓN: 29/01/2026
	VERSIÓN: 4		PÁGINA: 6-7
			REVISÓ Y APROBÓ: Comité CIGD No.1 de 2026.


- SEG-F-040 Cronograma de las actividades del plan de seguridad y privacidad de la información para la vigencia 2026
- Formato Plan de Acción de los Planes Institucionales y Estratégicos, Código: PLA-F-012.

6. DOCUMENTOS REFERENCIADOS

- ambit. (s.f.). Obtenido de.
- Concepto, E. (2013-2021). *Concepto.de*. Obtenido de <https://concepto.de/sistema-de-informacion/debitoor>. (s.f.). Obtenido de <https://debitoor.es/glosario/definicion-de-activo>
- Información, T. (s.f.). Obtenido de <https://www.tecnologias-informacion.com/integridaddatos.html>
- Varela, F. A. (s.f.). NovaSec. Obtenido de <https://www.novasec.co/blog/67-gestion-de-activos-de-informacion>
- VEGAGESTION. (s.f.). Obtenido de <https://vegagestion.es/cuales-las-principales-amenazas-la-seguridad-informatica/#:~:text=Robo%20de%20informaci%C3%B3n,o%20confidenciales%2C%20cambio%20de%20informaci%C3%B3n%E2%80%A6>

7. CONTROL DE MODIFICACIONES

VERSIÓN	FECHA	DESCRIPCIÓN DE LA MODIFICACION	RELIZADA POR
1	27/01/2023	Documento Nuevo	Ingeniera de Sistemas apoyo al proceso de las TIC's Líderes del proceso de Gestión de las TIC's
2	30/01/2024	Actualización del numeral 1 objetivo, dado que se actualizo la política de seguridad y privacidad de la información sufrió modificaciones Actualización del numeral 2 Alcance, dado que se actualizo la política de seguridad y privacidad de la información sufrió modificaciones Actualización del numeral 3, en el cual se incluyeron los responsables de acuerdo con los roles actuales del área Inclusión de componente autodiagnóstico numeral 5.1 Actualización del numeral 5.2 situación actual, dado que ya no existe la política de seguridad y privacidad	Elaboró: Ingeniero Oficial de Seguridad Informática y protección de datos. Revisó: Coordinador TI

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		FECHA ELABORACIÓN: 27/01/2023
	CÓDIGO: SEG-PL-006		FECHA ACTUALIZACIÓN: 29/01/2026
	VERSIÓN: 4		PÁGINA: 7-7
			REVISÓ Y APROBÓ: Comité CIGD No.1 de 2026.

		<p>de la información, ahora se llama política de seguridad de la información ciberseguridad y protección de la privacidad</p> <p>Actualización del numeral 5.4 actividades plan para la gestión sistemática y cíclica de riesgos de seguridad digital</p> <p>Actualización del numeral 5.3 Mapa de ruta</p> <p>Actualización del numeral 5.4 plan para la implementación del modelo de privacidad de la información y seguimiento a la política de seguridad de la información, ciberseguridad y protección de la privacidad- vigencia 2024.</p>	
3	30/01/2025	<p>Actualización numeral 2 alcance donde se relaciona la vigencia actual</p> <p>Actualización numeral 3 de los cargos del proceso de Gestión Tic</p> <p>Actualización del numeral 5.3 Mapa de ruta</p> <p>Actualización del numeral 5.4 plan para la implementación del modelo de privacidad de la información y seguimiento a la política de seguridad de la información, ciberseguridad y protección de la privacidad- vigencia 2025</p>	<p>Elaboró: Profesional especializada en seguridad y privacidad de la información</p> <p>Revisó: Profesional especializado de sistemas</p>
4	29/01/2026	<p>Actualización del numeral 5.4 plan para la implementación del modelo de seguridad y privacidad de la información</p>	<p>Elaboró: Profesional especializada en seguridad y privacidad de la información</p> <p>Revisó: Profesional especializado de sistemas</p>