

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		FECHA ELABORACIÓN: 27/01/2023
	CODIGO: SIS-PL-006		FECHA ACTUALIZACIÓN: 30/01/2024
	VERSION: 2		PAGINA: 0-7
			REVISO Y APROBÓ: Comité CIGD No. 2 de 2024.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN



2024

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		FECHA ELABORACIÓN: 27/01/2023
	CODIGO: SIS-PL-006		FECHA ACTUALIZACIÓN: 30/01/2024
	VERSION: 2		PAGINA: 1-7
			REVISO Y APROBÓ: Comité CIGD No. 2 de 2024.

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 2024	5
5.5	ANEXOS	6
6.	DOCUMENTOS REFERENCIADOS	6
7.	CONTROL DE MODIFICACIONES	7

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		FECHA ELABORACIÓN: 27/01/2023
	CODIGO: SIS-PL-006		FECHA ACTUALIZACIÓN: 30/01/2024
	VERSION: 2		PAGINA: 2-7
			REVISO Y APROBÓ: Comité CIGD No. 2 de 2024.

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 actualizada mediante la Resolución 0552 de 2023 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 2024.

3. RESPONSABLE:

Coordinador de TI, Ingeniero oficial de seguridad informática y protección de datos, Líder de infraestructura de TI y Líder de 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
	CODIGO: SIS-PL-006		FECHA ACTUALIZACIÓN: 30/01/2024
	VERSION: 2		PAGINA: 3-7
			REVISO Y APROBÓ: Comité CIGD No. 2 de 2024.

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

Para el periodo 2023, se ha llevado a cabo la ejecución completa de las actividades planificadas en el marco del Plan de Seguridad y Privacidad de la Información. Esto se ha logrado mediante la implementación efectiva de las fases de elaboración del plan correspondiente a dicha vigencia.

La publicación del plan ha sido un componente crucial para informar a la comunidad, colaboradores y entes de control sobre las medidas adoptadas. Se ha llevado a cabo una campaña de socialización y sensibilización que incluye dos sesiones anuales de sensibilización, así como píldoras informativas mensuales de la importancia de la seguridad de la información y las amenazas. Estas acciones buscan promover el conocimiento y la conciencia acerca de las políticas de seguridad de la información y la protección de datos personales.

Adicionalmente, se ha implementado un sistema de informes detallados sobre el análisis de amenazas detectadas por el firewall. Estos informes proporcionan una visión integral de las posibles vulnerabilidades, permitiendo tomar medidas correctivas de manera oportuna.

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

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		FECHA ELABORACIÓN: 27/01/2023
	CODIGO: SIS-PL-006		FECHA ACTUALIZACIÓN: 30/01/2024
	VERSION: 2		PAGINA: 4-7
			REVISO Y APROBÓ: Comité CIGD No. 2 de 2024.

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.

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 2024

5.3 MAPA DE RUTA

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN															
FASE	OBJETIVO	ACTIVIDAD	2024												MEDICIÓN Y SEGUIMIENTO
			ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC	Indicador
PLANIFICACIÓN	Establecer las actividades y procesos necesarios para cumplir con los requisitos de seguridad y privacidad de la información establecidos	Actualizar política de seguridad de la información en concordancia con la NTC ISO 27001:2022 dando cumplimiento al MSPi (modelo de seguridad y privacidad de la información)													Actividades ejecutadas Actividades Programadas
		Crear política, procedimientos, formatos y manuales complementarios a la política general de seguridad de la													

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		FECHA ELABORACIÓN: 27/01/2023
	CODIGO: SIS-PL-006		FECHA ACTUALIZACIÓN: 30/01/2024
	VERSION: 2		PAGINA: 5-7
			REVISO Y APROBÓ: Comité CIGD No. 2 de 2024.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN															
FASE	OBJETIVO	ACTIVIDAD	2024												MEDICIÓN Y SEGUIMIENTO
			ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC	Indicador
		información													
		Actualizar la política de Protección de Datos Personales de la ESE ISABU													
IMPLEMENTACIÓN	Ejecutar actividades, controles y medidas de protección que permitan la mitigación de riesgos de seguridad de la información.	Crear Cronograma de Capacitaciones de la política de seguridad de la información.													Actividades ejecutadas / Actividades Programadas
		Realizar Socialización de alineamientos de política de seguridad al personal de la institución de la ESE ISABU.													
		Ejecutar programa de monitoreo en seguridad de la información, Ciberseguridad y protección de la privacidad													
		Realizar simulacro de seguridad digital													
		Evaluar capacitaciones y Participación de funcionarios													
EVALUACIÓN DE DESEMPEÑO	Hacer seguimiento y medición a la implementación del MSPI.	Medir la efectividad de los controles y políticas definidas (Evaluar el resultado obtenido en las actividades y análisis realizadas)													Actividades ejecutadas / Actividades Programadas
		Revisar los niveles de riesgos.													

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 2024

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.	ACTIVIDAD	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	FORMATO
1	Actualizar política de seguridad de la información en concordancia con la NTC ISO 27001:2022 dando cumplimiento al MSPI (modelo de seguridad y privacidad de la información)	actualizar política de seguridad de la información, ciberseguridad y protección de la privacidad.	Ing. de Seguridad Informática y Protección de Datos.	Informe donde se relacione toda la documentación creada dando cumplimiento al MSPI
2	Realizar proceso de sensibilización de las políticas de seguridad de la información, ciberseguridad y protección de privacidad, así como la	Se Socializará La Política De Seguridad de la información, ciberseguridad y protección de la privacidad, así como la Política De Protección De Datos Personales, Por Medio	Ing. de Seguridad Informática y Protección de Datos.	* Informe de ejecución de socialización donde se evidencia la actividad y las actas de reunión y el control de asistencia.

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		FECHA ELABORACIÓN: 27/01/2023
			FECHA ACTUALIZACIÓN: 30/01/2024
	CODIGO: SIS-PL-006		PAGINA: 6-7
	VERSION: 2		REVISO Y APROBÓ: Comité CIGD No. 2 de 2024.

No.	ACTIVIDAD	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	FORMATO
	política de protección de datos personales.	De Capacitaciones, Sensibilización De Personal De La ESE ISABU.		
3	Realizar simulacro de seguridad digital	Realizar un simulacro por medio de una herramienta informática que permita simular de forma controlada un escenario de phishing	Ing. de Seguridad Informática y Protección de Datos.	* Informe de ejecución del simulacro
4	Realizar seguimiento trimestral al firewall corporativo para identificar eventos bloqueados y detectados que puedan interferir en la protección de la información.	Realizar seguimiento trimestral al firewall corporativo para identificar eventos bloqueados y detectados que puedan interferir en la protección de la información.	Líder de Infraestructura tecnológica	* Informe de seguimiento de firewall con periodicidad trimestral para la vigencia 2024
5	Realizar Análisis de riesgos de seguridad de la información de acuerdo al procedimiento de gestión de riesgos	Realizar Análisis de riesgos de seguridad de la información de acuerdo con el procedimiento de gestión de riesgos	Ingeniero de seguridad informática y protección de datos	* Informe anual de riesgos donde determina los riesgos residuales en zona moderada y alta que requieren tratamiento
6	Ejecutar programa de monitoreo en seguridad de la información ciberseguridad y protección de la privacidad	Hacer monitoreo del cumplimiento de las políticas de seguridad de la información y protección de datos mediante el procedimiento de monitoreo de seguridad de la información	Ingeniero de seguridad informática y protección de datos	* Informe semestral de ejecución de monitoreo a la seguridad de la información

Fuente: Oficina de Gestión de las TIC's

5.5 ANEXOS

Formato Plan de Acción Estratégico e Institucional, Código: PLA-F-012.

6. DOCUMENTOS REFERENCIADOS

- ambit. (s.f.). Obtenido de <https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas#:~:text=Una%20vulnerabilidad%20es%20un%20fallo,o%20un%20fallo%20de%20dise%C3%B1o.>
- 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>

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		FECHA ELABORACIÓN: 27/01/2023
	CODIGO: SIS-PL-006		FECHA ACTUALIZACIÓN: 30/01/2024
	VERSION: 2		PAGINA: 7-7
			REVISO Y APROBÓ: Comité CIGD No. 2 de 2024.

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 a 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 de la información, ahora se llama policita de seguridad de la información ciberseguridad y protección de la privacidad Actualización del numeral 5.4 actividades plan para la gestión sistemática y cíclica de riesgos de seguridad digital Actualización del numeral 5.3 Mapa de ruta 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.	Elaboró: Ingeniero Oficial de Seguridad Informática y protección de datos. Revisó: Coordinador TI