PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

E.S.E. ISABU Instituto de Salud de Bucaramanga

2023

CONTENIDO

1. OBJETIVO: 3
2. ALCANCE: 3
3. RESPONSABLE: 3
4. DEFINICIONES 3
5. DESARROLLO 4
   5.1 SITUACIÓN ACTUAL 4
   5.2 MAPA DE RUTA 5
   5.3 PLAN PARA LA IMPLEMENTACIÓN DEL MODELO DE PRIVACIDAD DE LA INFORMACIÓN Y SEGUIMIENTO A LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN - VIGENCIA 2023 6
   5.3.1. ANEXOS 6
6. DOCUMENTOS REFERENCIADOS 7
7. CONTROL DE MODIFICACIONES 7

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 y Privacidad de la Información actualizada mediante la Resolución 0565 de 2022 ESE ISABU, con el fin de asegurar el cumplimiento de la integridad, disponibilidad, legalidad 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 y privacidad de la información, 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 2023.

3. RESPONSABLE:

Lideres de proceso de Gestión de las Tic´s, Ingeniero Oficial de Seguridad Informática y Protección de Datos

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.

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

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

5.1 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 y Privacidad de la información. 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 incremente 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 informática:

- Integridad.
- Disponibilidad.
- Confidencialidad.

Así mismo, en atención tanto a lo especificado en la política de seguridad y privacidad de la información, como lo estipulado en el estándar NTC ISO 27001:2013, se aborda la identificación, valoración, tratamiento y gestión de riesgos de seguridad informática frente a ciber - amenazas, 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 el cuatrienio el cual a la fecha se dado cumplimiento al 100%.

5.2 MAPA DE RUTA

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN							
FASE	**OBJETIVO**	**ACTIVIDAD**	**2020**	**2021**	**2022**	**2023**	**MEDICIÓN Y SEGUIMIENTO**
							Indicador
PLANIFICACIÓN	Establecer las actividades y procesos necesarios para cumplir con los requisitos de seguridad y privacidad de la información establecidos	Establecer Políticas de Seguridad de la Información y Protección de Datos Personales					Actividades ejecutadas / Actividades Programadas
		Actualizar la política de seguridad de la información de la ISABU					
		Actualizar la política de Protección de Datos Personales de la ESE ISABU					
		Actualizar Manual Operativizaciones de la Política de Seguridad de la Información.					
		Realizar Contratación de un profesional que realice el seguimiento y monitoreo de las herramientas de seguridad de la información de la Institución.					
		Realizar la renovación de las licencias necesarias para los equipos de seguridad y respaldo.					
IMPLEMENTACIÓN	Ejecutar actividades, controles y medidas de protección que permitan la mitigación de riesgos de seguridad de la información.	Realizar Socialización de alineamientos de política de seguridad al personal de la institución de la ESE ISABU.					Actividades ejecutadas / Actividades Programadas
		Realizar seguimiento y gestión a sistemas de riesgos tecnológicos de la institución. (Informe del Firewall, que nos indica el número de intento de ingresos fraudulentos a nuestro sistema de información)					
		Crear Cronograma de Capacitaciones de la política de seguridad de la información.					
		Realizar seguimiento a las Políticas de: seguridad de la información y protección de datos.					
		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.					

		Actualizar los planes entorno a la seguridad de la información para la vigencia futura					

5.3 PLAN PARA LA IMPLEMENTACIÓN DEL MODELO DE PRIVACIDAD DE LA INFORMACIÓN Y SEGUIMIENTO A LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN - VIGENCIA 2023

Teniendo en cuenta las políticas seguridad y privacidad de la información Aprobado por la ESE ISABU, a continuación, se establece el Plan de seguridad y privacidad de la información; Enfocado desde la seguridad informática frente a las ciber-amenazas.

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

No.	ACTIVIDAD	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	FORMATO
1	Elaborar plan de seguridad y privacidad de la información para la vigencia 2023	Definir los lineamientos para la ejecución de las actividades del plan de seguridad y privacidad de la información	Ing. de Seguridad Informática y Protección de Datos.	Plan de seguridad y privacidad de la información
2	Publicar en página web institucional y socializar el plan de seguridad y privacidad de la información por correo electrónico.	Dar a conocer a la comunidad, colaboradores, entes de control el plan de seguridad y privacidad de la información de la ESE ISABU para la vigencia 2023	Ing. de Seguridad Informática y Protección de Datos.	Correo electrónico y link de página web institucional
3	Socializar las Políticas de Seguridad y Privacidad de la Información.	Se Socializará La Política De Seguridad Informáticas Y La Política De Protección De Datos Personales, Por Medio De Capacitaciones, Sensibilización De Personal De La ESE ISABU.	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.
4	Establecer los mecanismos de protección digital, para fortalecer la confidencialidad, integridad, disponibilidad y permitir implementar las políticas de seguridad de la información y protección de datos personales.	Realizar Actualización De Licencia Del Firewall e Informe de Firewall donde se evidencia el seguimiento y monitoreo en configuraciones y efectividad del software en cuanto a bloqueos y protección de datos e información.	Ingeniero De Seguridad Informática Y Protección De Datos	Informe de seguimiento de firewall con periodicidad trimestral para la vigencia 2023, se programan 4 entregables en el año
5	Realizar Seguimiento a las Políticas de Seguridad de La Información y Protección de Datos.	Hacer monitoreo del cumplimiento de las políticas de seguridad de la información y protección de datos mediante seguimiento y apoyo al grupo de Gobierno de seguridad y protección de datos personales.	Ingeniero de seguridad informática y protección de datos	* Informe semestral de ejecución de seguimiento las políticas de seguridad de la información y protección de datos personales, donde se evidencia la actividad, las actas de reunión y el control de asistencia.
6	Determinar los factores y/o aspectos a mejorar que hacen parte del MSPI	Actualización de Plan de Seguridad y Privacidad de la Información	Ingeniero de seguridad informática y protección de datos	* Documento - Plan Actualizado Para Siguiente Vigencia.

Fuente: Oficina de Gestión de las TIC´s

5.3.1. ANEXOS

- Formato Plan de Acción Estratégico 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

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