NIT. 800.084.206-2	SEGUIMIENTO A PLANES DE MEJORAMIENTO Y/O RECOMENDACIONES	FECHA ELABORACIÓN: 28-09-2020
		FECHA ACTUALIZACIÓN: 27/08/2021
	CODIGO: 1300-CIN-F-007	PAGINA: 1
	VERSION: 2	REVISO Y APROBÓ: Grupo Primario Control Interno

AUDITORIA O SEGUIMIENTO : Gestión TIC vigencia 2021

FECHA DE SEGUIMIENTO OFICINA DE CONTROL INTERNO: OCTUBRE DE 2022

HALLAZGO/ RECOMENDACIÓN N°.	DESCRIPCIÓN DEL HALLAZGO, PLAN DE MEJORA Y/O RECOMENDACIÓN	DESCRIPCIÓN DE LAS METAS (COMPROMISO)	FECHA INICIACIÓN DE LAS METAS	FECHA TERMINACIÓN DE LAS METAS	RESPONSABLE	SEGUIMIENTO Y EVALUACIÓN OCI	CUMPLIMIENTO %
1	• 1. No se evidencia un documento completo de la Política de Seguridad de la información, lo cual se soporta en la información documentada en el mapeo realizado, incumpliendo de esta forma con lo establecido en el control A.5.1.1 de la Norma ISO 27001:2013 y en el capítulo 5.2 Política de la Norma ISO 27001:2013.	• Informe de riesgos identificados	1/03/2022	31/05/2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	En el documento "INFORME DE RIESGOS IDENTIFICADOS" se evidencia los trabajos realizados para iniciar un Sistema de Seguridad de la Información, teniendo en cuenta los controles de la ISO 27001:2013 para lograr así tener un sistema actualizado para la protección de la información. En esta tarea se basaron en la detección de las vulnerabilidades que tiene la Oficina de Sistema en el ESE ISABU.	100%
		• Política actualizada con Resolución	junio de 2022	septiembre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Se esta actualizando el documento, para el mes de noviembre para su revisión en grupo primario y pasar a resolución a gerencia para firma.	0%
		• Publicación Política en Pag. Web •Cronograma de actividades para Socializar Política	1/010/2022	noviembre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
		• Informe de Seguimiento	diciembre de 2022	enero de 2023	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
2	2. No existen objetivos definidos formalmente en materia de seguridad de la información.	• Levantamiento de información de la situación actual • Valoración y Evaluación de riesgos en diferentes áreas, a partir de aplicar algunas encuestas y entrevistas, inspección visual	1/03/2022	31/05/2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	En el documento "INFORME DE RIESGOS IDENTIFICADOS", se evidencia los trabajos realizados, para definir correctamente los objetivos de SGSI. Se evidencia el levantamiento de información para definir los objetivos del sistema de gestión de seguridad de la información. Se están adelantando las entrevistas con las áreas con el fin de obtener la valoración y evaluación de los riesgos.	100%
		• Actualización de Política de seguridad de seguridad de la información.	junio de 2022	septiembre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Se esta actualizando el documento, para el mes de noviembre para su revisión en grupo primario y pasar a resolución a gerencia para firma.	0%
		• Publicar y Socializar Nueva Política de seguridad de la información	1/010/2022	noviembre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
		• Implementación de los mecanismos de control que se puedan realizar con recursos actuales de la ESE ISABU. • Realizar Seguimiento al cumplimiento de la política a los funcionarios de la ESE ISABU	diciembre de 2022	enero de 2023	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%

HALLAZGO/ RECOMENDACIÓN N°.	DESCRIPCIÓN DEL HALLAZGO, PLAN DE MEJORA Y/O RECOMENDACIÓN	DESCRIPCIÓN DE LAS METAS (COMPROMISO)	FECHA INICIACIÓN DE LAS METAS	FECHA TERMINACIÓN DE LAS METAS	RESPONSABLE	SEGUIMIENTO Y EVALUACIÓN OCI	CUMPLIMIENTO %
3	3. Se encontraron documentos que requieren actualización.	• Revisión y análisis de Documentos relacionados a la política de seguridad de la información	mayo de 2022	agosto de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Se presenta diagrama de tipología de red actualizado, sin embargo se encuentra en actualización y codificación algunos documentos como el manual de políticas de seguridad informática y manual de gestión de riesgos de seguridad digital.	0%
		• Actualización de Documentos	marzo de 2022	septiembre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Se esta actualizando el documento, para el mes de noviembre para su revisión en grupo primario y pasar a resolución a gerencia para firma.	0%
		• Revisión y Aceptación Grupo Primario	octubre de 2022	octubre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
		• Codificación Calidad	noviembre de 2022	diciembre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
4	4. No se realiza seguimiento, medición y evaluación de riesgos.	• Levantamiento de información de la situación actual • Valoración y Evaluación de riesgos en diferentes áreas, a partir de aplicar algunas encuestas y entrevistas, inspección visual	1/03/2022	31/05/2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	En el documento "INFORME DE RIESGOS IDENTIFICADOS" se evidencia la implantación de un Sistema de Gestión de la Seguridad de la Información (SGSI) que requiere de un conocimiento profundo de la Gestión de Riesgos. Es importante que con el levantamiento realizado de las vulnerabilidades y los próximos trabajos, la identificación de los activos de información, se pueda tener la capacidad de eliminar el riesgo, transferir el riesgo, asumir el riesgo y mitigar el riesgo, situación que se ve reflejada en el informe presentado. Se encuentra en construcción la matriz de riesgos.	100%
		• Actualización de Política de seguridad de la información.	junio de 2022	septiembre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	El documento se encuentra en actualización y codificación por parte de la oficina de calidad	0%
		• Publicar y Socializar Nueva Política de seguridad de la información	1/010/2022	noviembre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
		• Implementación de los mecanismos de control que se puedan realizar con recursos actuales de la ESE ISABU. • Realizar Seguimiento al cumplimiento de la política a los funcionarios de la ESE ISABU	diciembre de 2022	enero de 2023	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%

HALLAZGO/ RECOMENDACIÓN N°.	DESCRIPCIÓN DEL HALLAZGO, PLAN DE MEJORA Y/O RECOMENDACIÓN	DESCRIPCIÓN DE LAS METAS (COMPROMISO)	FECHA INICIACIÓN DE LAS METAS	FECHA TERMINACIÓN DE LAS METAS	RESPONSABLE	SEGUIMIENTO Y EVALUACIÓN OCI	CUMPLIMIENTO %
5	5. No se evidencia un documento con las responsabilidades, deberes y contactos para la seguridad de la información, lo cual afecta en Funciones y áreas de responsabilidad que puedan presentar algún conflicto de interés y deben estar separadas para reducir la posibilidad de que se presenten incidentes relacionados, por ejemplo, con modificaciones no autorizadas o involuntarias, así como mal uso de los activos, lo cual se soporta en la información documentada en el mapeo realizado, incumpliendo de esta forma con lo establecido en el control A.6.1.1 – A.6.1.2 – A.6.1.3 de la Norma ISO 27001:2013	• Levantamiento de información de la situación actual • Valoración y Evaluación de riesgos en diferentes áreas, a partir de aplicar algunas encuestas y entrevistas, inspección visual	1/03/2022	31/05/2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	El área de las TICS de la ESE ISABU realizó el levantamiento de la información, de igual manera se realizó la valoración y evaluación del riesgo en diferentes áreas. Teniendo en cuenta que el levantamiento esta adelantado, recomienda esta oficina que es necesario que se tenga en cuenta que en el Sistema de Gestión de Seguridad de la Información, es importante asumir un rol, un individuo tiene la responsabilidad de alcanzar ciertos objetivos trazados, las responsabilidades determinadas para cada rol dependerán de las metas establecidas para las diferentes actividades. Con el levantamiento de información de las vulnerabilidades, se detecta los roles y responsabilidades en la Oficina de Sistemas y las que se deben tener en cuenta para el SGSI, como por ejemplo el Responsable de la Seguridad de la Información, Equipo del Proyecto y el Comité de Seguridad entre otros.	100%
		• Actualización de Política de seguridad de seguridad de la información.	junio de 2022	septiembre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
		• Publicar y Socializar Nueva Política de seguridad de la información	1/010/2022	noviembre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
		• Realizar Seguimiento al cumplimiento de la política a los funcionarios de la ESE ISABU	diciembre de 2022	enero de 2023	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
6	6. No se evidencia plan de educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo, incumpliendo de esta forma con lo establecido en el control A.7.2.2 – A.7.2.3 de la Norma ISO 27001:2013.	• Crear Cronograma de Capacitaciones de la política de seguridad de la información.	1/010/2022	noviembre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
		• Reuniones virtuales organizados por grupos, para crear sensibilización en seguridad de la información • Presentaciones, que se enviaran por correo electrónico con una retroalimentación para ver el resultado. • Protectores de pantalla que recuerden medidas de seguridad básicas.	diciembre de 2022	mayo de 2023	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
		Evaluar capacitaciones y Participación de funcionarios	mayo de 2023	junio de 2023	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
		Establecer acciones a base de los resultados obtenidos	julio de 2023	septiembre de 2023	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%

HALLAZGO/ RECOMENDACIÓN N°.	DESCRIPCIÓN DEL HALLAZGO, PLAN DE MEJORA Y/O RECOMENDACIÓN	DESCRIPCIÓN DE LAS METAS (COMPROMISO)	FECHA INICIACIÓN DE LAS METAS	FECHA TERMINACIÓN DE LAS METAS	RESPONSABLE	SEGUIMIENTO Y EVALUACIÓN OCI	CUMPLIMIENTO %
7	• 7. No se han realizado actividades de formación o toma de conciencia en el año 2021 en materia de Seguridad de la Información, incumpliendo de esta forma con lo establecido en el control A.7.2.2.	• Crear Cronograma de Capacitaciones de la política de seguridad de la información.	1/010/2022	noviembre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
		• Reuniones virtuales organizados por grupos, para crear sensibilización en seguridad de la información • Presentaciones, que se enviaran por correo electrónico con una retroalimentación para ver el resultado. • Protectores de pantalla que recuerden medidas de seguridad básicas.	diciembre de 2022	mayo de 2023	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
		Evaluar capacitaciones y Participación de funcionarios	mayo de 2023	junio de 2023	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
		Establecer acciones a base de los resultados obtenidos	julio de 2023	septiembre de 2023	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
8	8. No se evidencia un documento donde se identifica los activos de la organización, lo cual se soporta en la información documentada en el mapeo realizado, incumpliendo de esta forma con lo establecido en el control A.8.1 de la Norma ISO 27001:2013.	• Levantamiento de información de la situación actual • Valoración y Evaluación de riesgos en diferentes áreas, a partir de aplicar algunas encuestas y entrevistas, inspección visual • Análisis y requerimiento herramienta de software para inventarios de activos informáticos	marzo de 2022	agosto de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	La oficina de sistemas realizó el levantamiento de información, evidenciando documento denominado " informe de riesgos identificados" del cual se desprende el mapa de riesgos de gestión. De igual manera se realizó la valoración y evaluación de riesgos en las diferentes áreas. Para evidenciar el trabajo realizado se presenta formato de encuesta con cada uno de las áreas. Gestion TIC realiza el análisis de la herramienta de software para inventarios de activos informáticos, implementando software libre GLPI	100%
		• Revisión de inclusión al inventario general de la ESE ISABU Los equipos físicos informáticos y los software licenciados en el sistema.	marzo de 2022	noviembre de 2022	•Jefe Oficina de Planeación •Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
		• Evaluar el resultado obtenido en las actividades y análisis realizadas	noviembre de 2022	diciembre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
		• Establecer Acciones con base a los resultados	enero de 2023	marzo de 2023	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
		• Levantamiento de información de la situación actual	marzo de 2022	agosto de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	En el informe de" riesgos identificados" numeral 3.7 vulnerabilidades en administración de equipos de computo, se puede identificar los diferentes riesgos en los equipos de computo con los medios informáticos extraíbles.	100%

HALLAZGO/ RECOMENDACIÓN N°.	DESCRIPCIÓN DEL HALLAZGO, PLAN DE MEJORA Y/O RECOMENDACIÓN	DESCRIPCIÓN DE LAS METAS (COMPROMISO)	FECHA INICIACIÓN DE LAS METAS	FECHA TERMINACIÓN DE LAS METAS	RESPONSABLE	SEGUIMIENTO Y EVALUACIÓN OCI	CUMPLIMIENTO %
9	• 9. No se evidencia gestión en el manejo de los medios informáticos.(cintas, discos, removibles, informes impresos) para evitar la revelación, modificación, eliminación o destrucción no autorizadas de la información almacenada en los medios, incumpliendo de esta forma con lo establecido en el control A.8.3.1 - A.8.3.2 de la Norma ISO 27001:2013	• Creación de proceso para la clasificación de la información, donde se incluirá la gestión de los medios informáticos, disposición , procedimiento para la autorización y control de entrada y salida de elementos que contengan información de propiedad de la entidad y que protección se tiene para garantizar la confidencialidad.	marzo de 2022	noviembre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
		• Revisión y Aceptación Grupo Primario	noviembre de 2022	diciembre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
		• Codificación Calidad	enero de 2023	marzo de 2023	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
10	• 10. No se evidencia la clasificación de la información en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizadas, incumpliendo de esta forma con lo establecido en el control A.8.2.1 de la Norma ISO 27001:2013.	• Levantamiento de información de la situación actual	marzo de 2022	agosto de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	En el informe de" riesgos identificados" numeral 3.7 vulnerabilidades en administración de equipos de computo, se identifica los diferentes riesgo sobre la falta de respaldo de la información.	100%
		• Creación de proceso para la clasificación de la información, donde se incluirá la gestión de los medios informáticos, disposición , procedimiento para la autorización y control de entrada y salida de elementos que contengan información de propiedad de la entidad y que protección se tiene para garantizar la confidencialidad.	marzo de 2022	noviembre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
		• Revisión y Aceptación Grupo Primario	noviembre de 2022	diciembre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
		• Codificación Calidad	enero de 2023	marzo de 2023	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
		• Levantamiento de información de la situación actual • Valoración y Evaluación de riesgos en diferentes áreas, a partir de aplicar algunas encuestas y entrevistas, inspección visual	1/03/2022	31/05/2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	El área de las TICS realizó el levantamiento de la información, diagnosticando y realizando una evaluación, evidenciándolo en el documento "INFORME DE RIESGOS IDENTIFICADOS". Se recomienda que debe establecer, documentar y revisar con periodicidad una política de control de acceso, teniendo en cuenta los requisitos de la ESE ISABU para los activos a su alcance.	100%

HALLAZGO/ RECOMENDACIÓN N°.	DESCRIPCIÓN DEL HALLAZGO, PLAN DE MEJORA Y/O RECOMENDACIÓN	DESCRIPCIÓN DE LAS METAS (COMPROMISO)	FECHA INICIACIÓN DE LAS METAS	FECHA TERMINACIÓN DE LAS METAS	RESPONSABLE	SEGUIMIENTO Y EVALUACIÓN OCI	CUMPLIMIENTO %
11	• 11. No se evidencia la implementación de Política de Control de Acceso, se debería establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información, incumpliendo de esta forma con lo establecido en el control A.9.1.1 – A.9.1.2 – A.9.2 de la Norma ISO 27001:2013.	• Actualización de Política de seguridad de seguridad de la información.	junio de 2022	septiembre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	La política de seguridad de la información se encuentra en actualización y a la espera de codificación por parte de la oficina de Calidad.	0%
		• Publicar y Socializar Nueva Política de seguridad de la información	1/010/2022	noviembre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
		• Implementación de los mecanismos de control que se puedan realizar con recursos actuales de la ESE ISABU. • Realizar Seguimiento al cumplimiento de la política a los funcionarios de la ESE ISABU	diciembre de 2022	enero de 2023	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
14	• 14. No se evidencia que los equipos estén protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro eléctrico, incumpliendo de esta forma con lo establecido en el control A.11.2.1 - A.11.2.2 de la Norma ISO 27001:2013	• Levantamiento de información de la situación actual • Valoración y Evaluación de riesgos en diferentes áreas, a partir de aplicar algunas encuestas y entrevistas, inspección visual	1/03/2022	31/05/2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	El área de las TICS realiza el levantamiento de la información y la valoración de lo evidenciado, quedando consignado en el documento "INFORME DE RIESGOS IDENTIFICADOS" lo mencionado. Se recomienda verificar las fallas eléctricas para la planificación de las acciones a seguir para mitigar esta situación.	100%
		• Actualización de Política de seguridad de seguridad de la información.	junio de 2022	septiembre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	El centro de computo esta protegido con una UPS y ciertas estaciones de trabajo cuentan con UPS para salvaguardar la información durante el fallo electrico. Dentro del Manual de la política de seguridad de la información se encuentra en el numeral 6.7.1 que cada equipo de computo debe estar protegido con un respaldo de energía. Sin embargo la política de seguridad de la información se encuentra en actualización y a la espera de codificación por parte de la oficina de Calidad.	0%
		• Publicar y Socializar Nueva Política de seguridad de la información	1/010/2022	noviembre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
		• Implementación de los mecanismos de control que se puedan realizar con recursos actuales de la ESE ISABU. • Realizar Seguimiento al cumplimiento de la política a los funcionarios de la ESE ISABU	diciembre de 2022	enero de 2023	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
		• Levantamiento de información de la situación actual	marzo de 2022	julio de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Se evidencia el informe de levantamiento de las necesidades de puntos de Red de la ESE ISABU. Se tener planificado iniciar el estudio de mercado para generar un presupuesto para esta actividad.	100%

HALLAZGO/ RECOMENDACIÓN N°.	DESCRIPCIÓN DEL HALLAZGO, PLAN DE MEJORA Y/O RECOMENDACIÓN	DESCRIPCIÓN DE LAS METAS (COMPROMISO)	FECHA INICIACIÓN DE LAS METAS	FECHA TERMINACIÓN DE LAS METAS	RESPONSABLE	SEGUIMIENTO Y EVALUACIÓN OCI	CUMPLIMIENTO %
15	• 15. Se ve expuesto el cableado de telecomunicaciones que transmite datos que sirve de soporte a los servicios de información, incumpliendo de esta forma con lo establecido en el control A.11.2.3 de la Norma ISO 27001:2013.	Actualización de Política de seguridad incluyendo en ella los controles para poder implementa y Creación de necesidad para contratación y ejecución.	junio de 2022	marzo de 2023	• Dirección Administrativa • Jefe Oficina de Planeación • Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
		Revisión y validación de ejecución	junio de 2023	febrero de 2024	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
		Establecer acciones a base de los resultados obtenidos	febrero de 2024	abril de 2024	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
16	• 16. No se evidencia el aseguramiento de la disponibilidad e integridad de todos los equipos (planes de contingencia), incumpliendo de esta forma con lo establecido en el control A.11.2.4 de la Norma ISO 27001:2013	• Revisión y análisis de Documentos relacionados a la política de seguridad de la información	mayo de 2022	agosto de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	En el informe de riesgos identificados se relaciona en el numeral 2 se identifican los principales riesgos de infraestructura. Este insumo es importante para la actualización de la política de seguridad de la información.	100%
		• Actualización de Documentos	marzo de 2022	septiembre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	La política de seguridad de la información se encuentra en actualización y a la espera de codificación por parte de la oficina de Calidad	0%
		• Revisión y Aceptación Grupo Primario	octubre de 2022	octubre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
		• Codificación Calidad	noviembre de 2022	diciembre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
17	• 17. No se evidencia procedimientos para asegurar los equipos desatendidos, incumpliendo de esta forma con lo establecido en el control A.11.2.8 – A.11.2.9 A.9.1.2 de la Norma ISO 27001:2013.	• Revisión y análisis de Documentos relacionados a la política de seguridad de la información	mayo de 2022	agosto de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	En el informe de riesgos identificados se relaciona en el numeral 3.7 vulnerabilidades en la administración de equipos de computo se relaciona el riesgo de no activar el bloqueo de pantalla.	100%
		• Actualización de Documentos	marzo de 2022	septiembre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Se esta implementando política por el Directorio Activo con bloqueo de pantalla, pero hace falta la socialización para bloquear definitivamente la sesión de trabajo de los usuarios cuando no están en su puesto de trabajo, que se encuentra en el manual de la política de seguridad de la información numeral 6.3.1 y 6.7.2 que se encuentra en proceso de actualización y codificación por parte de la oficina de calidad.	100%

HALLAZGO/ RECOMENDACIÓN N°.	DESCRIPCIÓN DEL HALLAZGO, PLAN DE MEJORA Y/O RECOMENDACIÓN	DESCRIPCIÓN DE LAS METAS (COMPROMISO)	FECHA INICIACIÓN DE LAS METAS	FECHA TERMINACIÓN DE LAS METAS	RESPONSABLE	SEGUIMIENTO Y EVALUACIÓN OCI	CUMPLIMIENTO %
		• Revisión y Aceptación Grupo Primario	octubre de 2022	octubre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
		• Codificación Calidad	noviembre de 2022	diciembre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
18	• 18. No se evidencia un seguimiento al control de cambios, incumpliendo de esta forma con lo establecido en el control A.12.1.2 de la Norma ISO 27001:2013.	• Revisión y análisis de Documentos relacionados a la política de seguridad de la información	mayo de 2022	agosto de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	En el informe de riesgos identificados se relacionó en los numerales 3.1 vulnerabilidad de servidores el análisis de los documentos. De igual manera en el numeral 3.5 vulnerabilidad de los aplicativos .	100%
		• Actualización de Documentos	marzo de 2022	septiembre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	En el manual de la política de seguridad de la información se relaciona en los numerales 6.7.1, 6.7.3, 6.7.4.y 6.7.5 el seguimiento a control de cambios, este documento se encuentra en actualización y codificación por parte de la oficina de calidad.	100%
		• Revisión y Aceptación Grupo Primario	octubre de 2022	octubre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
		• Codificación Calidad	noviembre de 2022	diciembre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
19	• 19. No se evidencia separación de ambientes de pruebas y operación, para reducir los riesgos de acceso no autorizado o los cambios del sistema en producción, incumpliendo de esta forma con lo establecido en el control A.12.1.4 de la Norma ISO 27001:2013.	• Levantamiento de información de la situación actual • Valoración y Evaluación de riesgos en diferentes áreas, a partir de aplicar algunas encuestas y entrevistas, inspección visual	1/03/2022	31/05/2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	En el documento "INFORME DE RIESGOS IDENTIFICADOS" se evidencia el levantamiento de las vulnerabilidades de los Servidores y el Data Center, se recomienda que es importante tener un ambiente de pruebas para las aplicaciones que están en funcionamiento en la ESE ISABU.	100%
		• Actualización de Política de seguridad de seguridad de la información.	junio de 2022	septiembre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	En el manual de la política de seguridad de la información se relaciona en los numerales 6.7.3 y 6.7.4. se relaciona la separación de los ambientes de prueba y operación, este documento se encuentra en actualización y codificación por parte de la oficina de calidad.	0%
		• Publicar y Socializar Nueva Política de seguridad de la información	1/010/2022	noviembre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
		• Implementación de los mecanismos de control que se puedan realizar con recursos actuales de la ESE ISABU. • Realizar Seguimiento al cumplimiento de la política a los funcionarios de la ESE ISABU	diciembre de 2022	enero de 2023	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%

HALLAZGO/ RECOMENDACIÓN N°.	DESCRIPCIÓN DEL HALLAZGO, PLAN DE MEJORA Y/O RECOMENDACIÓN	DESCRIPCIÓN DE LAS METAS (COMPROMISO)	FECHA INICIACIÓN DE LAS METAS	FECHA TERMINACIÓN DE LAS METAS	RESPONSABLE	SEGUIMIENTO Y EVALUACIÓN OCI	CUMPLIMIENTO %
20	• 20. No se evidencia gestión de la capacidad para supervisar y ajustar la utilización de los recursos, así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido del sistema, incumpliendo de esta forma con lo establecido en el control A.12.1.3 de la Norma ISO 27001:2013.	• Levantamiento de información de la situación actual • Valoración y Evaluación de riesgos en diferentes áreas, a partir de aplicar algunas encuestas y entrevistas, inspección visual	1/03/2022	31/05/2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	En el documento "INFORME DE RIESGOS IDENTIFICADOS" se evidencia el levantamiento de la información, siendo este informe un insumo Importante realizar la Gestión de la Capacidad para proyectar el crecimiento de la Oficina de Sistemas	100%
		• Actualización de Política de seguridad de seguridad de la información.	junio de 2022	septiembre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	En el manual de la política de seguridad de la información en le numeral 6.7.4 se identifica la política de monitorear y ajustar el uso de los recursos tecnológicos. La política se encuentra en actualización y codificación por parte de calidad.	0%
		• Publicar y Socializar Nueva Política de seguridad de la información	1/010/2022	noviembre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
		• Implementación de los mecanismos de control que se puedan realizar con recursos actuales de la ESE ISABU. • Realizar Seguimiento al cumplimiento de la política a los funcionarios de la ESE ISABU	diciembre de 2022	enero de 2023	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
21	• 21. No se evidencia la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades, incumpliendo de esta forma con lo establecido en el control A.16 de la Norma ISO 27001:2013.	• Revisión y análisis de Documentos relacionados a la política de seguridad de la información	mayo de 2022	agosto de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	En el manual de la política de seguridad de la información se relaciona en los numerales 5.1.1., 5.1.2, 5.1.3 y 5.1.4 las políticas frente a la gestión de incidentes de seguridad, esta política se encuentra en actualización y codificación de calidad.	0%
		• Actualización de Documentos	marzo de 2022	septiembre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	En el manual de la política de seguridad de la información se relaciona en los numerales 5.1.1., 5.1.2, 5.1.3 y 5.1.4 las políticas frente a la gestión de incidentes de seguridad, esta política se encuentra en actualización y codificación de calidad.	0%
		• Revisión y Aceptación Grupo Primario	octubre de 2022	octubre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
		• Codificación Calidad	noviembre de 2022	diciembre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
22	• 22. En los contratos con personal y contratistas no se observan instrucciones en materia de manejo de reportes de debilidades y vulnerabilidades,	• Informe de riesgos identificados	1/03/2022	31/05/2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	En el documento "INFORME DE RIESGOS IDENTIFICADOS" se evidencia el levantamiento de los activos, es importante en la Oficina Jurídica plantear el tema para aplicar los controles establecidos en la ISO 27001:2013 mencionar una clausula referente con la Seguridad de la Información.	100%
		• Política actualizada con Resolución	junio de 2022	septiembre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	En la política de seguridad de la información se relaciona en los numerales 5.1.3 , 5.1.4. y 6.2 se emiten las directrices al respecto. La política se encuentra en actualización y codificación por parte de la oficina de calidad.	100%

HALLAZGO/ RECOMENDACIÓN N°.	DESCRIPCIÓN DEL HALLAZGO, PLAN DE MEJORA Y/O RECOMENDACIÓN	DESCRIPCIÓN DE LAS METAS (COMPROMISO)	FECHA INICIACIÓN DE LAS METAS	FECHA TERMINACIÓN DE LAS METAS	RESPONSABLE	SEGUIMIENTO Y EVALUACIÓN OCI	CUMPLIMIENTO %
	incumpliendo de esta forma con lo establecido en el control A.16.1.2.	• Publicación Política en Pag. Web • Cronograma de actividades para Socializar Política	1/010/2022	noviembre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
		• Informe de Seguimiento	diciembre de 2022	enero de 2023	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
23	• 23. No se evidencia que la organización determina sus necesidades de seguridad de la información y de continuidad para la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre, incumpliendo de esta forma con lo establecido en el control A.17.1.1	• Revisión y análisis de Documentos relacionados a la política de seguridad de la información	mayo de 2022	agosto de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	En el informe de identificación de riesgos, se relacionan el riesgo de desastres en el numeral 2 de riesgos de infraestructura.	100%
		• Actualización de Documentos	marzo de 2022	septiembre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	En la política de seguridad de la información se relaciona en los numerales 6.7.3 y 6.7.4 se emiten los lineamientos para el tratamiento ante desastres. Esta política se encuentra en actualización y codificación por parte de calidad.	0%
		• Revisión y Aceptación Grupo Primario	octubre de 2022	octubre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
		• Codificación Calidad	noviembre de 2022	diciembre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
24	• 24. Se evidencia la falta de licenciamiento de software Microsoft office en algunos equipos.	Levantamiento de Información y situación actual	1/03/2022	31/05/2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	En el documento “INVENTARIO LICENCIAS OFFICE” se evidencia el inventario realizado. Esta actividad se debe tener un alto grado de eficiencia y eficacia ya que el control de licenciamiento es muy neurálgico para la ESE ISABU.	100%
		Realizar necesidad para la contratación y ejecución	junio de 2022	agosto de 2022	•Jefe Oficina de Planeación •Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Se evidencia necesidad y contrato 763-2022 cuyo objeto es "compraventa de licencia, elementos informáticos y de respaldo eléctrico para las diferentes dependencias de la ESE ISABU". Se adquirieron: 20 licencias de Windows PRO10 75 licencias office	100%
		Revisión e instalación y pruebas de licencias activas	septiembre de 2022	noviembre de 2022	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
		Realizar seguimiento al Licenciamiento de Software	diciembre de 2022	febrero de 2023	•Coordinador Oficina de Sistemas •Ingeniero de seguridad de la información y de protección de datos	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%

HALLAZGO/ RECOMENDACIÓN N°.	DESCRIPCIÓN DEL HALLAZGO, PLAN DE MEJORA Y/O RECOMENDACIÓN	DESCRIPCIÓN DE LAS METAS (COMPROMISO)	FECHA INICIACIÓN DE LAS METAS	FECHA TERMINACIÓN DE LAS METAS	RESPONSABLE	SEGUIMIENTO Y EVALUACIÓN OCI	CUMPLIMIENTO %
25	• 25. PANACEA, se evidencia: • Mal funcionamiento o configuración en varios módulos de PANACEA, lo que afecta los procesos que adelante el funcionario responsable de su ejecución o administración • Se identifica un riego en recurso humano ya que un solo ingeniero da soporte a toda la entidad.	• Informe de análisis de inconsistencias y reportes frecuentes del Software - recopilar todos los inconvenientes y requerimientos (nomina – inventarios – web citas)	1/02/2022	31/05/2022	•Coordinador Oficina de Sistemas •Ingeniero Administrador de BD	En el documento "INFORME DE ANALISIS PANACEA - INCONSISTENCIAS Y REPORTES FRECUENTES DEL SOFTWARE" Se realiza un primer barrido de lo requerimientos por parte de los usuarios de PANACEA con su soporte para lograr un alto grado de satisfacción de su funcionamiento.	100%
		• Reuniones técnicas con los líderes de los procesos que actúan en PANACEA • Cronograma de Fortalecimiento y Capacitaciones para funcionarios de la ESE ISABU. •Informe de Necesidad de: Soporte del Software por parte del proveedor , Y Necesidad de contratación Ing. Apoyo en la gestión y administración de la base de datos	febrero de 2022	jun-22	•Coordinador Oficina de Sistemas •Ingeniero Administrador de BD	1. En el desarrollo de mejora para la aplicación PANACEA se han realizado reuniones para su mejoramiento y específicamente para CITAS WEB y su respectiva cotización. Horario de disponibilidad y número de contacto dirigido a las Direcciones Técnicas y líderes de proceso y parametrización de los usuarios y se deja constancia que no todo el personal debe tener permiso para la descarga de historias clínica, solo visualizar en caso que sea necesario. 2. Se requieres un cronograma de capacitación 3. Se evidencia la gestión de la necesidad del Soporte Técnico por parte de CNT Sistemas de información S.A.S y su puesta en marcha. 4. Es importante resaltar que la auditoria de Gestión TIC 2021 resulto efectiva en la necesidad de un soporte en la administración del software PANACEA, teniendo como consecuencia la contratación del ingeniero Líder de Sistemas y el ingeniero de sistemas para apoyar a la oficina de sistemas en el manejo del sistema CNT panacea de la ese ISABU.	100%
		•Actas de Reuniones con proveedor y con Usuarios que utilizan el Software •Actas de Capacitaciones •Evidencia de Evaluaciones de Actividades	jul-22	oct-22	•Coordinador Oficina de Sistemas •Ingeniero Administrador de BD	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%
		realizar seguimiento de mejora y realizar recomendaciones	nov-22	dic-22	•Coordinador Oficina de Sistemas •Ingeniero Administrador de BD	Esta actividad se encuentra dentro de los tiempos estipulados para su cumplimiento.	0%

Fecha de publicación página web institucional:

Jefe Oficina de Gestión y Control Interno

Apoyó seguimiento: Profesional de apoyo control interno