1100-380-10
CI - 169

Firma_____
Radicado: **00003290**
Enviado: 18/08/2023 - 10:18 a.m.
ventanillaunica
ESE ISABU

Bucaramanga, 18 de agosto de 2023

Doctor
GERMAN JESUS GÓMEZ LIZARAZO
Gerente

Doctora
CARMEN CECILIA RINCÓN CONTRERAS
Subgerente Administrativa

Ingeniero
WILLIAM FIGUEROA PINEDA
Profesional especializado - Sistemas
ESE ISABU
Bucaramanga

Asunto: Informe final de auditoría al Proceso Gestión de las TICS

Cordial saludo:

La Oficina de Control Interno de la E.S.E. ISABU, en desarrollo de sus funciones y conforme al plan de auditorías para la vigencia 2023, presenta informe final de la auditoría realizada al proceso Gestión de las TICS para su conocimiento y fines pertinentes.

Teniendo en cuenta que se generaron hallazgos los cuales fueron aceptados, se debe presentar a esta oficina, el plan de mejoramiento dentro de los diez (10) días hábiles siguientes al recibo de la presente comunicación.

Agradezco su atención.

SILVIA JULIANA PINZÓN CUEVAS
Jefe Oficina de Control Interno

P/E: Vianey González Gamarra
Profesional de apoyo control interno

Revisó: Silvia Juliana Pinzón Cuevas
Jefe Oficina de Control Interno

AUDITORIA DE PROCESO Y/O SUBPROCESO: GESTIÓN DE LAS TICS

FECHA DE INICIO: 01 de julio de 2023

FECHA DE FINALIZACIÓN: 18 de agosto de 2023

RESPONSABLES DEL PROCESO: Dra. Carmen Cecilia Rincón Contreras
Subgerente Administrativa
Ing. William Figueroa Pineda
Profesional Especializado -Sistemas

ALCANCE:

Evaluar y verificar el proceso de Gestión de las TICS, en los siguientes temas:

- ✓ Temas abordados en la Evaluación de desempeño institucional FURAG.
- ✓ En Comité Institucional de Coordinación de Control Interno, celebrado el 14 de junio de 2023, los miembros de forma unánime decidieron acceder a la solicitud de Planeación – Sistemas de ajustar las actividades y trasladar los hallazgos No. 9,15,20,21,22 y 23 a la auditoria de gestión TICS que se apertura, por lo tanto, y en virtud de la decisión adoptada por el Comité, la auditoria iniciará con la revisión y aprobación por parte de la oficina de control interno de las actividades correspondiente a los hallazgos mencionados.
- ✓ Procesos y Procedimientos aplicados por la gestión TICS
- ✓ Planes institucionales MIPG: Política de Seguridad Digital y Gobierno Digital

OBJETIVOS:

Evaluar de manera independiente y objetiva el proceso de las TICS, con el fin de identificar oportunidades de mejora que contribuyan al cumplimiento de la misión y los objetivos institucionales de manera eficiente y eficaz.

MARCO NORMATIVO:

- Constitución política de Colombia, artículos 209 y 269.
- Ley 87 de 1993, "Por la cual se establecen normas para el ejercicio del control interne en las entidades y organismos del Estado y se dictan otras disposiciones."
- Decreto 1008 del 14 de junio de 2018 "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único reglamentario del sector de las Tecnologías de la Información y las Comunicaciones".
- Ley 1341 de 2009 "Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones — TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones".
- Documento CONPES 3650 del 15 de marzo de 2010 Importancia Estratégica de Ia Estrategia de Gobierno en Línea.
- Ley 1712 de 2014 "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones." Documentos internos del área de TICS

VISITAS Y ENTREVISTAS REALIZADAS:

En el marco de la auditoría, se realizaron entrevistas al líder del proceso y personal de apoyo en las siguientes fechas 26/07/2023, 08/03/2023, 04/08/2023, 09/08/2023.

Igualmente se llevaron a cabo las siguientes actividades:

- Revisión y verificación documental de las evidencias entregadas por el personal entrevistado.
- Revisión y verificación de los procesos y procedimientos que aplican al área de las TICS.

ACEPTACIÓN O NO ACEPTACIÓN DEL HALLAZGO:

La oficina de Control Interno de la E.S.E. ISABU, en cumplimiento de sus funciones, Plan Anual de Auditoría basado en riesgos de la vigencia 2023 y en el marco del MIPG, presenta informe final de auditoría realizado al proceso de Gestión de las TICS.

La presente auditoría se llevó a cabo en atención a las normas y técnicas de auditoría, e incluyó las evidencias que dan fe del proceso auditado y el cumplimiento de las disposiciones legales.

Comentario de la oficina de Control Interno: La presente auditoria se limitó a la verificación documental del proceso, debido a la falta de un auditor especializado o con conocimientos específicos en el área de sistemas.

➢ PROCESOS Y PROCEDIMIENTOS

Con respecto al proceso y sus procedimientos, se observan los siguientes relacionados a la gestión TICS:

CARACTERIZACIÓN	FECHA
PROCESO GESTIÓN DE LAS TICS	18/06/2019
PROCEDIMIENTOS	
GIF-P-006 PROCEDIMIENTO GESTIÓN DE LAS TECNOLOGIAS DE LA INFORMACIÓN	7/07/2022
GIF-P-007 PROCEDIMIENTO DE IDENTIFICACION, GESTION Y CLASIFICACION DE ACTIVOS DE INFORMACIÓN E INFRAESTRUCTURA CRITICA DE TI	30/03/2023
P-3900-01 PROCEDIMIENTO LICENCIAMIENTO DE EQUIPOS DE COMPUTO	18/06/2019
P-3900-02 PROCEDIMIENTO EVALUACION, SOPORTE Y MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE HARDWARE	18/06/2019
P-3900-03 PROCEDIMIENTO SOPORTE Y MANTENIMIENTO DE LOS SERVIDORES	18/06/2019
P-3900-04 PROCEDIMIENTO DE SOLICITUD DE INFORMACIÓN	25/10/2020
SIS-P-008 PROCEDIMIENTO GESTIÓN DEL CAMBIO	19/05/2023
SIS-P-009 PROCEDIMIENTO DE MONITOREO Y SEGUIMIENTO DE SEGURIDAD DE LA INFORMACIÓN	19/05/2023
GUIAS	
GIF-G-001 GUIA DE USABILIDAD DEL SISTEMA DE INFORMACIÓN	19/05/2023
GIF-G-002 GUIA DE LA METODOLOGIA DEL SISTEMA DE INFORMACIÓN	7/07/2022
SIS-G-003 GUÍA INFRAESTRUCTURA TECNOLÓGICA DE LAS TECNOLOGÍAS DE LA INFORMACIÓN	7/03/2023
MANUALES	
M-3600-01 MANUAL DE GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL	23/06/2020
FORMATOS	

GIF-F-022 Matriz de identificación, gestión y clasificación de activos de información e infraestructura critica de TI	30/03/2023
SIS-F-002 REGISTRO SOPORTE	23/02/2022
SIS-F-003 CONTACTO PERSONAL SISTEMAS	23/02/2022
SIS-F-023 FORMATO DE GESTIÓN DEL CAMBIO	19/05/2023
SIS-F024 MATRIZ DE OBSERVACIONES MONITOREO Y SEGUIMIENTO DE SEGURIDAD DE LA INFORMACIÓN	19/05/2023
SIS-F025 PROGRAMA DE MONITOREO Y SEGUIMIENTO DE SEGURIDAD DE LA INFORMACION	19/05/2023
DOCUMENTOS DE APOYO	
PLAN	
PL-3600-02 PLAN DE CONTINGENCIA INFORMATICA	21/08/2020
SIS-PL-001 PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION-PETI	28/02/2022
SIS-PL-003 PLAN DE DISPONIBILIDAD DE LOS SERVICIOS TICS EN LA ESE ISABU EN HORARIOS CONVENCIONALES, NOCTURNOS, FINES DE SEMANA Y FESTIVOS	23/02/2022
SIS-PL-004 PLAN DE CONTINGENCIA ANTE NO FUNCIONAMIENTO DE HISTORIA CLINICA ELECTRONICA	30/08/2022
SIS-PL-005 PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL	27/01/2023
SIS-PL-006 PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	27/01/2023
SIS-PL-007 PLAN DE MANTENIMIENTO DE EQUIPOS DE CÓMPUTO, DISPOSITIVOS DE RED Y SERVIDORES	25/01/2023
SIS-PL-008 PLAN PARA LA GESTIÓN SISTEMÁTICA Y CÍCLICA DE RIESGOS DE SEGURIDAD DIGITAL	25/01/2023
SIS-PL-009 PLAN DE ASEGURAMIENTO DE LA CALIDAD DEL SISTEMA DE INFORMACIÓN	27/01/2023
POLITICA	
GIF-PO-001 POLÍTICA TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y LUCHA CONTRA LA CORRUPCIÓN	29/04/2022
GIF-PO-002 POLÍTICA GOBIERNO DIGITAL	29/04/2022
GIF-PO-003 POLÍTICA SEGURIDAD DIGITAL	29/04/2022
RES.0342 POLITICA DE SEGURIDAD DE LA INFORMACION	13/12/2017

Hallazgo No. 1

Condición: En la auditoría realizada se procedió a verificar la aplicabilidad, vigencia y pertinencia de las actividades contenidas en los procedimientos, evidenciándose actualización de cuatro (4) procedimientos, a saber: Procedimiento Gestión de la tecnologías de la información, Procedimiento de identificación, gestión y clasificación de activos de información e infraestructura critica de TI, Procedimiento Gestión del Cambio y Procedimiento de Monitoreo y Seguimiento de Seguridad de la Información.

Pese a lo antes señalado, algunos documentos de apoyo, manuales y procedimientos del área se encuentran desactualizados, como son: Procedimiento de licenciamiento de equipos de cómputo, Procedimiento de evaluación, soporte y mantenimiento preventivo y correctivo de Hardware, Procedimiento soporte y mantenimiento de servidores, procedimiento de solicitud de información, plan de contingencia informática, plan de contingencia ante no funcionamiento de historia clínica electrónica, política transparencia, acceso a la información pública y lucha contra la corrupción y la política de la seguridad de la información (2017).
Criterio: Procedimientos correspondientes al proceso de Gestión de las TICS, lo cuales proporcionan una guía para las operaciones diarias, aseguran el cumplimiento de la normatividad y

orientación para la toma de decisiones y simplifican los procesos internos

Causa: Ausencia de control, seguimiento, aplicabilidad y actualización de los procedimientos documentados en el proceso de Gestión de las TICS.

Consecuencia: Desconocimiento por parte del personal del proceso TICS en la aplicación de los procedimientos del área.

El presente hallazgo se identificó en los siguientes procedimientos:

- PROCEDIMIENTO LICENCIAMIENTO DE EQUIPOS DE COMPUTO

El punto No. 4 del procedimiento describe “Se ingresa el CD en el equipo y se hace el registro de compra de la licencia en la página web de cada programa”.

Esta actividad actualmente se encuentra desactualizada, ya que la licencia se activa realiza en la página del proveedor.

Igualmente, el procedimiento se debe actualizar al formato vigente establecido por el área de calidad.

- PROCEDIMIENTO EVALUACIÓN, SOPORTE Y MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE HARDWARE

El procedimiento genera confusión al incorporar actividades de mantenimiento preventivo y correctivo.

Las actividades de mantenimiento preventivo ya no se realizan de acuerdo a este procedimiento ya que se tiene un plan de mantenimiento de equipos de cómputo, dispositivos de red y servidores.

Teniendo en cuenta lo anterior se sugiere ajustar el procedimiento de mantenimiento correctivo.

El procedimiento se debe actualizar al formato vigente establecido por el área de calidad.

PROCEDIMIENTO SOPORTE Y MANTENIMIENTO DE SERVIDORES

En la actividad de recepción de solicitud, no se describen los medios por los cuales se deben recibir

las solicitudes, siendo necesario definir los canales de comunicación.

El procedimiento se debe actualizar al formato vigente establecido por el área de calidad.

- PROCEDIMIENTO SOLICITUD DE INFORMACIÓN

En el procedimiento se habla solo de solicitud, pero dentro de las actividades se menciona la posibilidad de modificar la información. Se confunde el procedimiento entre el nombre y las actividades descritas.

El procedimiento se debe actualizar al formato vigente establecido por el área de calidad.

OPORTUNIDAD DE MEJORA: En la revisión realizada se detectó que en el listado maestro de documentos de gestión de las TICS se relacionan procedimientos que no pertenecen al área. Por lo tanto, es necesario que las TICS realice junto a la oficina de Calidad, una actualización y depuración del listado maestro de documentos.

Hallazgo No. 2

Condición: Al aplicar los procedimientos de evaluación, soporte y mantenimiento preventivo y correctivo de hardware y el procedimiento de soporte y mantenimiento de servidores en la visita realizada a la Gestión de las TICS, esta oficina de control interno evidenció que no se cuenta con un archivo físico o electrónico (hoja de vida), en donde se lleve control efectivo y consolidado por equipos de cómputo y servidores, que brinde información relevante como: información del usuario (nombre del usuario, cargo, área y responsable del equipo), información de adquisición (tiempo de garantía, entidad o proveedor, fabricante), información del equipo (tipo, modelo, marca y serie, numero de inventario, IP, monitor, hardware, entre otros).

Lo anterior es de vital importancia con el fin que cada equipo de cómputo y servidor cuente con un registro, memoria y trazabilidad histórica que le permita a las TICS la toma de decisiones acertadas respecto a bajas, mantenimientos o adquisiciones.

Criterio: Procedimiento de evaluación, soporte y mantenimiento preventivo y correctivo de hardware y el procedimiento de soporte y mantenimiento de servidores.

Causa: Ausencia de control, seguimiento y aplicabilidad de los procedimientos documentados en el proceso de Gestión de las TICS.

Consecuencia: Inefectividad en el trabajo y actividades propias de Gestión de las TICS.

- **TALENTO HUMANO**

El proceso Gestión de las TICS cuenta con el siguiente personal para el desarrollo de sus actividades:

NÚMERO DE CONTRATO	OBJETO CONTRATO	CARGO	VINCULACIÓN		LUGAR DE TRABAJO
			CPS	PP	
	PROFESIONAL ESPECIALIZADO (Sistemas)	Profesional Especializado (sistemas)		X	HLN
0249-2023	PRESTACION DE SERVICIOS PROFESIONALES COMO INGENIERO LIDER DE SISTEMAS DE INFORMACION DE LA ESE ISABU	Líder Sistema de la Información	X		HLN
0095-2023	PRESTACION DE SERVICIOS PROFESIONALES COMO INGENIERO LIDER DE INFRAESTRUCTURA INFORMATICA DE LA ESE ISABU	Líder Infraestructura Tecnológica	X		HLN
0088-2023	PRESTAR SERVICIOS PROFESIONALES COMO INGENIERO DE SISTEMA COMO APOYO A LA OFICINA DE SISTEMAS DE LA ESE ISABU	Apoyo Profesional Sistemas	X		HLN

0829-2023	PRESTAR SERVICIOS PERSONALES DE APOYO A LA GESTION EN EL AREA DE SISTEMAS DE LA ESE ISABU	Apoyo sistema de la Información	X		HLN
0798-2023	PRESTACION DE SERVICIOS PROFESIONALES COMO INGENIERO DE SISTEMAS PARA APOYAR A LA OFICINA DE SISTEMAS EN EL MANEJO DEL SISTEMA DE INFORMACION CNT PANACEA DE LA ESE ISABU.	Apoyo sistema de la Información	X		HLN
0828-2023	PRESTACION DE SERVICIOS COMO TECNOLOGO DE APOYO A LA GESTION EN EL AREA DE SISTEMAS DE LA ESE ISABU	Tecnólogo - Soporte Técnico	X		HLN -UIMIST - CS
0171-2023	PRESTACION DE LOS SERVICIOS PERSONALES COMO TECNICO DE SISTEMAS A LA GESTION EN EL AREA DE SISTEMAS DE LA ESE ISABU	Técnico - Soporte	X		HLN - CS
0213-2023	PRESTACION DE LOS SERVICIOS PERSONALES COMO TECNICO DE SISTEMAS EN LA GESTION EN EL AREA DE SISTEMAS DE LA ESE ISABU	Técnico - Soporte	X		UIMIST - CS
0165-2023	PRESTACION DE SERVICIOS PERSONALES COMO TECNICO DE SISTEMAS A LA GESTION EN EL AREA DE SISTEMAS DE LA ESE ISABU	Técnico - Soporte	X		HLN - UIMIST - CS
0599-2023	PRESTAR SERVICIOS PROFESIONAL ESPECIALIZADOS EN SEGURIDAD DE LA INFORMACIÓN, SEGURIDAD DIGITAL y OFICIAL DE PROTECCIÓN DE DATOS PERSONALES SEGÚN LEY 1581 DEL 2012 PARA LA ESE ISABU	Profesional oficial de seguridad	X		HLN

Fuente: Información suministrada por el líder del proceso Gestión TICS.

En la revisión realizada por el equipo auditor se pudo evidenciar que el personal se encuentra operando y con las actividades a desarrollar definidas.

- **EVALUACION INDEPENDIENTE DEL SISTEMA DE CONTROL INTERNO – ACTIVIDADES DE CONTROL**

Dada la articulación del MIPG y el MECI, a través de la Séptima Dimensión denominada “Control Interno”, componente “Monitoreo y seguimiento”, el cual señala la importancia de adelantar acciones frente a la aplicación de evaluaciones continuas y/o independientes para determinar la existencia y operación de los componentes del Sistema de Control Interno, la oficina de control interno desarrolló un cuestionario con el fin de verificar temas referentes al sistema de control interno y que es importante tratar en la presente auditoría:

1. **La entidad establece actividades de control relevantes sobre las infraestructuras tecnológicas; los procesos de gestión de la seguridad y sobre los procesos de adquisición, desarrollo y mantenimiento de tecnologías.**

   Respuesta Gestión TICS: La entidad tiene establecida la Política de Seguridad de la Información, Política de Seguridad y Protección de Datos Personales, Política de Gobierno Digital, Plan Estratégico de las Tecnologías, Información y las Comunicaciones - PETIC, gestión de la Capacidad (política que está en construcción), plan de mantenimiento preventivo anual,

todos ellos publicados en la página web institucional www.isabu.gov.co

2. **Para los proveedores de tecnología selecciona y desarrolla actividades de control internas sobre las actividades realizadas por el proveedor de servicios.**

   Respuesta Gestión TICS: La entidad cuenta con el manual de contratación para los procesos contractuales.
   Los profesionales responsables del área de tecnología de la información apoyan en la evaluación técnica de los proveedores que se presentan para llevar a cabo la fase precontractual del proceso de contratación y en un segundo momento apoyan en la supervisión técnica en la ejecución de las actividades contractuales del proveedor o contratista del servicio. La supervisión se realiza de acuerdo con el informe mensual mediante informe de actividades enviado por el proveedor junto con cuenta de cobro el cual debe ser aprobado por el supervisor del contrato y el apoyo del supervisor.

3. **Se cuenta con matrices de roles y usuarios siguiendo los principios de segregación de funciones.**

   Respuesta Gestión TICS: Se cuenta con matrices de roles de usuarios en el sistema de información Panacea, cada usuario del sistema de información tiene su rol o permiso, se encuentra documentado a través de los procedimientos del Proceso de Gestión de las TIC, en la política de seguridad, en la guía de usabilidad del Sistema de Información.

Observación:

Conforme a lo anterior la entidad dentro del ambiente de control, ha desarrollado actividades que contribuyen a la mitigación de los riesgos y su implementación permite el logro de los objetivos institucionales.

RECOMENDACIÓN: Teniendo en cuenta lo anterior, esta oficina de control interno recomienda continuar con la implementación de las diferentes actividades que permitan el fortalecimiento del proceso de Gestión de las TIC y la mejora continua del proceso.

- **FORMULARIO ÚNICO DE REPORTES Y AVANCES DE GESTIÓN (FURAG)**

La Oficina de Control Interno, como tercera línea de defensa del MIPG realizó verificación de una serie de temas consignados en el Formulario Único de Reporte de avances de la Gestión FURAG, que guardan relación a la implementación de la política de Gobierno Digital y Seguridad Digital.

1. **¿Qué actividades de innovación llevó a cabo la entidad en la vigencia 2023 basadas en el enfoque experimental y haciendo uso de las TIC? ¿Qué beneficios se han obtenido y quienes fueron los beneficiarios?**

Respuesta Gestión de las TICS: Se adquirió el Chatbot para el Call Center, buscando mejorar la atención y servicio de los usuarios. Se anexa como soporte Contrato con la Empresa COMUNICACIONES GANA TODO APP SAS cuyo objeto es “Prestar de manera cumplida los servicios de implementación y alquiler de la plataforma para manejo de WhatsApp empresarial para

centralizar y mejorar la atención de clientes" y Acta de entrega de fecha 22/06/2023.

2. **¿La entidad ha adoptado las fases de planeación, implementación y pruebas de funcionalidad de IPv6?**

Respuesta Gestión de las TICS: NO, solo nos encontramos en fase de Planeación. La institución actualmente utiliza el protocolo IPV4. Se anexa como soporte PLAN DE DIRECCIONAMIENTO IPV6 – ESE ISABU.

3. **¿La entidad está registrada en la Tienda Virtual del Estado Colombiano (TVEC)?**

Respuesta Gestión de las TICS: Si, aunque esto es administrado por el área de Jurídica.

4. **Capacitación en temáticas de la Política de Gobierno Digital durante la vigencia 2023: a quienes?**

Respuesta Gestión de las TICS: Durante el primer semestre se realizó sensibilización tanto para el grupo Directivo de la institución como para el personal administrativo y asistencial, Según cronograma establecido para la actual vigencia. Así como el envío de la capsulas mensuales para mantener el personal informado. Se anexa como soporte: Informe de sensibilización primer semestre 2023.

5. **La política de seguridad y privacidad de la información de la entidad: ¿Está formulada, aprobada, implementada y se actualiza mediante un proceso de mejora continua?**

Respuesta Gestión de las TICS: Si, Está formulada, aprobada, implementada y se actualiza mediante un proceso de mejora continua. Se relaciona link de publicación de política en la Página Web https://isabu.gov.co/wp-content/uploads/2022/12/RESOLUCION- No-0565-DE-2022.-1.pdf.

6. **Con respecto al inventario de activos de seguridad y privacidad de la información de la entidad: ¿el inventario está aprobado, clasificado y se actualiza mediante el proceso de mejora continua?**

Respuesta Gestión de las TICS: Si, Está formulada, aprobada, implementada y se actualiza mediante un proceso de mejora continua. Se adjunta GIF-F-022 Matriz de identificación, gestión y clasificación de activos de información e infraestructura critica de TI.

7. **Con respecto a los riesgos de seguridad y privacidad de la información de la entidad: Los identificó, están aprobados, se implementó un proceso para valorarlos y se actualizan mediante un proceso de mejora continua.**

Respuesta Gestión de las TICS: Si, Se identificó, están aprobados, se implementó un proceso para valorarlos y se actualizan mediante un proceso de mejora continua. Se anexa como soportes: Se creó y se adjunta como evidencia el PLAN-DE-TRATAMIENTO-DE-RIESGO-DE -SEGURIDAD-DIGITAL-2023.

8. **¿La entidad implementó el plan de tratamiento de riesgos de seguridad de la información?**

Respuesta Gestión de las TICS: Si, Plan de Tratamiento de Riesgos de Seguridad digital. Se creó y se adjunta como evidencia el PLAN-DE-TRATAMIENTO-DE-RIESGO-DE-SEGURIDAD-DIGITAL-2023.

9. **¿La entidad realizó análisis de vulnerabilidades de seguridad a los activos de información (hardware, software, aplicaciones, redes) en la vigencia 2023?**

Respuesta Gestión de las TICS: Si, Pero se realizó de manera interna no se hizo con una entidad externa. Se adjunta Informe de vulnerabilidades e inscripción de CSIRT activa.

10. **¿La entidad realizó pruebas de recuperación de información y continuidad de los sistemas de información críticos en la vigencia 2023?**

Respuesta Gestión de las TICS: Si, se realizó Pruebas de restauración de la base de datos, para garantizar la copia de manera efectiva para responder a situaciones de interrupción o desastre que puedan afectar la disponibilidad. Se adjunta actas de Ejecución de pruebas de restauración de la vigencia 2023.

11. **Trámites total o parcialmente en línea.**

Respuesta Gestión de las TICS: Citas web es una herramienta electrónica, utilizada para ejecutar tramites de asignación de citas en línea utilizado por el área de subcientifica –asistencial - Call center.

12. **Trámites total o parcialmente en línea que cumplen con todos los criterios de accesibilidad web, definidos en el anexo 1 de la Resolución MinTIC 1519 de 2020**.

Respuesta Gestión de las TICS: Como tramites en línea, actualmente tenemos el servicio de agendamiento de citas, con el módulo de la página institucional, cumpliendo con la resolución y anexo 1. Se relaciona el link: https://isabu.gov.co/

13. **¿Cuáles proyectos se tienen de transformación digital?**

Respuesta Gestión de las TICS: El chat Bot- utilizado para el mejoramiento del servicio en el Call Center para la asignación de citas. Se adjunta link del módulo de Citas web. Publicado en página web oficial de la institución: http://181.60.135.85/Cnt.Panacea.Web.CitasWeb/Account/Ingreso.aspx

Observación de Control Interno: De acuerdo con lo anterior, se pudo evidenciar que el proceso de las TICS viene realizando las diferentes gestiones para la implementación de las políticas de Gobierno Digital y Seguridad Digital, en pro del mejoramiento continuo y en cumplimiento de los parámetros normativos establecidos en la materia.

Conscientes que el proceso de transformación tecnológica comporta la adopción de un sinnúmero de directrices y que estas deben desarrollarse con el debido cuidado y con las herramientas disponibles, se recomienda continuar con las diferentes acciones para el fortalecimiento de las Políticas Institucionales en la E.S.E ISABU.

➢ PLANES INSTITUCIONALES MIPG 2023

La Oficina de Control Interno realizó comprobación del estado de la implementación de los diferentes planes institucionales que competen a las TICS (6 planes institucionales), a partir de la información del seguimiento a los planes institucionales realizado por la Oficina Asesora de Planeación e igualmente la información suministrada por el área de Sistemas.

- SEGUIMIENTO AL PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACIÓN (PETI)

El Plan Estratégico de Tecnologías de La Información (PETI) tiene como objetivo "Establecer el Plan Estratégico de Tecnología de la Información (PETI), que permita garantizar la adecuada administración de los recursos tecnológicos, infraestructura de datos, que faciliten el cumplimiento de la meta. Articulando de manera estratégica los planes, la visión y objetivos institucionales planteados en el plan de desarrollo de la ESE ISABU"

Para la vigencia 2023 el plan comprende la realización de 5 actividades con un total de 19 productos entregables de los cuales se observa con corte a 30 de junio de 2023 el cumplimiento del plan del 52% como se muestra a continuación:

PLAN	META ACTIVIDAD	INDICADOR META ACTIVIDAD	ACTIVIDAD DE TRABAJO	PRODUCTO / ENTREGABLE	RESPONSABLE	META EJECUTADA	META /ACTIVIDAD PROGRAMADA	RESULTADO META	CUMPLMIENTO DEL PLAN
PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	100%	Número de actividades ejecutadas (4) / Número de actividades programadas (4)	Crear cronograma y ejecutar los 3 mantenimientos preventivos programados para la vigencia actual	1. Un cronograma de mantenimiento anual. 2. Tres informes de mantenimiento preventivo anual con una periodicidad cuatrimestral de los 3 mantenimientos programados y ejecutados con el registro de la cantidad y descripción de equipos.	Líder de Infraestructura Tecnologica	2	4	0,50	52%
PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	100%	Número de actividades ejecutadas (5) / número de actividades programadas (5)	Ejecución de reposición y adquisición de equipos tecnológicos	1. Informe necesidad 2. ficha técnica 3. informe valor promedio de cotizaciones (estudios previos) 4. Copia de contrato 5. Informe de instalación y configuración de equipos y puesta en marcha.	Líder de Sistemas de información – Líder de Infraestructura Tecnologica	3	5	0,60	
PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	100%	Número de actividades ejecutadas (4) / Número de actividades programadas (4)	Ejecución de actualizaciones y mejoras del software panacea	1. Informe de gestión y análisis mejoramiento del software panacea – (actualizaciones, mejoras) 2. Informe y análisis de ejecución de la proyecto telemedicina según reunión pasadas solo se implementara en el HLN	Líder de Sistemas de información	2	4	1	
PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	100%	Número de actividades ejecutadas (3) / número de actividades programados (3)	Ejecución de adquisición de software para el sistema de gestión de riesgos, indicadores y de gestión integral.	1. Informe necesidad 2. Copia de contrato 3. Informe de instalación y configuración de equipos y puesta en marcha.	Líder de Sistemas de información	2	3	1	
PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	100%	Número de actividades eejecutadas (3) / número de actividades programados (3)	Ejecución e implementar herramienta tecnológica que permita mantener conversaciones con el usuario final, de forma automatizada y sencilla para la asignación de citas.	1. Informe necesidad 2. Copia de contrato 3. Informe de implementación	Líder de Sistemas de información	1	3	0	

Fuente: Oficina Asesora de Planeación

- SEGUIMIENTO AL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El plan de tratamiento de riesgos de seguridad y privacidad de la información tiene como objetivo "Establecer un Plan de tratamiento de riesgo de seguridad digital a través del cual se mitiguen las vulnerabilidades y amenazas asociados a los activos de información de la ESE ISABU, con el fin de lograr niveles de aceptación razonable del riesgo en relación con los atributos de disponibilidad, integridad y confidencialidad de la información de la entidad"

Para la vigencia 2023 el plan comprende la realización de 6 actividades con un total de 12 productos entregables de los cuales se observa con corte a 30 de junio de 2023 el cumplimiento del plan del 61% como se muestra a continuación:

PLAN	META ACTIVIDAD	INDICADOR META ACTIVIDAD	ACTIVIDAD DE TRABAJO	PRODUCTO / ENTREGABLE	RESPONSABLE	META EJECUTADA	META /ACTIVIDAD PROGRAMAD	RESULTADO META	CUMPLMIENTO DEL PLAN
PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	1	Plan de tratamiento de riesgos de seguridad aprobado	Elaborar Plan de tratamiento de riesgos de seguridad digital para la vigencia 2023	Plan de tratamiento de riesgos de seguridad aprobado	Ingeniero de seguridad informática y protección de datos	1	1	1	61%
PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	1	Publicar en página web institucional y socializar el Plan de tratamiento de riesgos de seguridad digital	Publicar en página web institucional y socializar el Plan de tratamiento de riesgos de seguridad digital por correo electrónico.	Correo electrónico y link de página web institucional	Ingeniero de seguridad informática y protección de datos	1	1	1	
PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	3	Número actividades ejecutadas / Total de Actividades programadas *100%	Establecer las actividades y procesos necesarios para cumplir con los requisitos de seguridad y privacidad de la información establecidos en el MSPI	1. Un cronograma de sensibilización y capacitación en seguridad de la información 2. Dos informes como evidencia a la implementación del programa de sensibilización y capacitación en seguridad de la información.	Ingeniero de seguridad informática y protección de datos	2	3	1	
PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	2	Número de informes prese	Ejecutar actividades, controles y medidas de protección que permitan la mitigación de riesgos de seguridad de la información	Informe semestral de seguimiento de copias de seguridad a la base de datos y servidores	Ingeniero de seguridad informática y protección de datos	1	2	1	
PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	4	Número de informes prese	Ejecutar actividades, controles y medidas de protección que permitan la mitigación de riesgos de seguridad de la información	Informe de seguimiento de antivirus con periocidad trimestral para la vigencia 2023, se programan 4 entregables en el año	Ingeniero de seguridad informática y protección de datos / Líder de Infraestructura	2	4	0,50	
PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	1	Plan e tratamiento de riesgos de seguridad y privacidad de la información actualizado	Determinar los factores y/o aspectos a mejorar que hacen parte del MSPI	Plan de tratamiento de riesgos de seguridad y privacidad de la información actualizado para la vigencia 2024.	Ingeniero de seguridad informática y protección de datos / Líder de Infraestructura	0	1	0	

Fuente: Oficina asesora de planeación

SEGUIMIENTO AL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El plan de seguridad y privacidad de la información tiene como 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".

Para la vigencia 2023 el plan comprende la realización de 6 actividades con un total de 11 productos entregables de los cuales se observa con corte a 30 de junio de 2023 el cumplimiento del plan del 58% como se muestra a continuación:

PLAN	META ACTIVIDAD	INDICADOR META ACTIVIDAD	ACTIVIDAD DE TRABAJO	PRODUCTO / ENTREGABLE	RESPONSABLE	META EJECUTADA	META /ACTIVIDAD PROGRAMADA	RESULTADO META	CUMPLMIENTO DEL PLAN
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	1	plan de seguridad y privacidad de la información aprobado.	Elaborar plan de seguridad y privacidad de la información para la vigencia 2023	Plan de seguridad y privacidad de la información, aprobado.	Ingeniero de seguridad informática y protección de datos	1	1	1	58%
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	1	Link de publicación y socialización del plan seguridad y privacidad de la información	Publicar en página web institucional y socializar el plan de seguridad y privacidad de la información por correo electrónico.	Correo electrónico y link de página web institucional	Ingeniero de seguridad informática y protección de datos	1	1	1	
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	2	Número de socializaciones	Socializar las Políticas de Seguridad y Privacidad de la Información.	Informe de ejecución de socialización donde se evidencia la actividad y las actas de reunión y el control de asistencia.	Ingeniero de seguridad informática y protección de datos	1	2	1	
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	4	Informes de seguimiento p	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.	Informe de seguimiento de firewall con periodicidad trimestral para la vigencia 2023.	Ingeniero de seguridad informática y protección de datos Líder de Infraestructura	2	4	0,50	
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	2	Informes de seguimiento p	Realizar Seguimiento a las Políticas de Seguridad de la Información 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.	Ingeniero de seguridad informática y protección de datos	1	2	1	
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	1	Plan de seguridad y privacidad de la información actualizado	Determinar los factores y/o aspectos a mejorar que hacen parte del MSPI	Plan de seguridad y privacidad de la información actualizado para la vigencia 2024	Ingeniero de seguridad informática y protección de datos	0	1	0	

Fuente: Oficina asesora de planeación

- SEGUIMIENTO AL PLAN DE ASEGURAMIENTO DE LA CALIDAD DEL SISTEMA DE LA INFORMACIÓN

El plan de aseguramiento de la calidad del sistema de la información tiene como objetivo "Implementar el Plan de aseguramiento de la calidad del sistema de información para la gestión de TI; en la ESE Instituto de salud de Bucaramanga basado en los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones Min Tic. requeridas para garantizar el buen funcionamiento del sistema de información de PANACEA".

Para la vigencia 2023 el plan comprende la realización de 5 actividades con un total de 8 productos entregables de los cuales se observa con corte a 30 de junio de 2023 el cumplimiento del plan del 80% como se muestra a continuación:

PLAN	META ACTIVIDAD	INDICADOR META ACTIVIDAD	ACTIVIDAD DE TRABAJO	PRODUCTO / ENTREGABLE	RESPONSABLE	META EJECUTADA	META /ACTIVIDAD PROGRAMADA	RESULTADO META	CUMPLMIENTO DEL PLAN
PLAN DE ASEGURAMIENTO DE LA CALIDAD DEL SISTEMA DE INFORMACIÓN	1	plan de aseguramiento de la calidad del sistema de información aprobado.	Elaborar plan de aseguramiento de la calidad del sistema de información para la vigencia 2023	Plan de aseguramiento de la calidad del sistema de información aprobado.	Proceso Gestión de las TIC'S	1	1	1	80%
PLAN DE ASEGURAMIENTO DE LA CALIDAD DEL SISTEMA DE INFORMACIÓN	1	Link de publicación y socialización del plan aseguramiento de la calidad del sistema de información	Publicar en página web institucional y socializar el plan aseguramiento de la calidad del sistema de información con el grupo de trabajo de la oficina de las TIC´s.	Acta de reunión y link de la página web institucional	Proceso Gestión de las TIC'S	1	1	1	
PLAN DE ASEGURAMIENTO DE LA CALIDAD DEL SISTEMA DE INFORMACIÓN	2	Informes presentados	Ejecutar instalaciones de nuevas versiones y parches de seguridad para el sistema de información PANACEA.	Informe con la evidencia del correo enviado sobre la ventana de mantenimiento para la instalación del parche y la descripción del caso o casos soluciones con esta actualización. (Aplica solo para los parches). Si la actualización es completa este informe llevara los casos de uso utilizados en el entorno de pruebas y los resultados obtenidos.	Proceso Gestión de las TIC'S	1	2	1	
PLAN DE ASEGURAMIENTO DE LA CALIDAD DEL SISTEMA DE INFORMACIÓN	2	Informes presentados	Modificar las plantillas de historias clínicas según requerimiento del comité de Historias Clínicas.	Informe de entrega de las modificaciones de la plantilla de historia clínica al comité de Historias clínicas.	Proceso Gestión de la TIC´S con apoyo del Comité de Historias Clínicas.	1	2	1	
PLAN DE ASEGURAMIENTO DE LA CALIDAD DEL SISTEMA DE INFORMACIÓN	2	Informes presentados	Validar los usuarios y perfiles creados en el sistema de información PANACEA de acuerdo a reporte de los líderes de proceso.	Informe con la relación de la depuración de usuarios del sistema de información PANACEA.	Proceso Gestión de las TIC'S con apoyo de los líderes de procesos.	2	2	1	

Fuente: Oficina asesora de planeación

- SEGUIMIENTO AL PLAN PARA LA GESTIÓN SISTEMÁTICA Y CÍCLICA DE RIESGOS DE SEGURIDAD DIGITAL

El plan para la gestión sistemática y cíclica de riesgos de seguridad digital tiene como objetivo "Analizar la práctica y gestión de riesgos de seguridad digital en el cual se logren identificar las amenazas y vulnerabilidades a las que la Institución pueda estar expuesta desde el un entorno cibernético, con el fin de fortalecer el ambiente de control y metodología de gestión de riesgos basados en Modelo Nacional de Gestión de Riesgos de Seguridad Digital (MGRSD) del Mintic".

Para la vigencia 2023 el plan comprende la realización de 4 actividades con un total de 4 productos entregables de los cuales se observa con corte a 30 de junio de 2023 el cumplimiento del plan del 50% como se muestra a continuación:

PLAN	META ACTIVIDAD	INDICADOR META ACTIVIDAD	ACTIVIDAD DE TRABAJO	PRODUCTO / ENTREGABLE	RESPONSABLE	META EJECUTADA	META /ACTIVIDAD PROGRAMADA	RESULTADO META	CUMPLMIENTO DEL PLAN
PLAN PARA LA GESTIÓN SISTEMÁTICA Y CÍCLICA DE RIESGOS DE SEGURIDAD DIGITAL	1	Un informe realizado	Realizar Análisis de Riesgos de TI	Informe de análisis de riesgos	Ingeniero oficial de seguridad informática y protección de datos	1	1	1	50%
PLAN PARA LA GESTIÓN SISTEMÁTICA Y CÍCLICA DE RIESGOS DE SEGURIDAD DIGITAL	1	Un link de Campus virtual	Fortalecer los controles orientados a la mitigación de los riesgos de la seguridad digital de la Institución.	Link de Campus virtual	Ingeniero oficial de seguridad informática y protección de datos	1	1	1	
PLAN PARA LA GESTIÓN SISTEMÁTICA Y CÍCLICA DE RIESGOS DE SEGURIDAD DIGITAL	1	Un informe realizado	Realizar análisis de vulnerabilidades en la Infraestructura de TI	Informe de análisis de vulnerabilidades en la Infraestructura de TI	Ingeniero oficial de seguridad informática y protección de datos Apoyo de Líder de Infraestructura tecnológica.	0	1	0	
PLAN PARA LA GESTIÓN SISTEMÁTICA Y CÍCLICA DE RIESGOS DE SEGURIDAD DIGITAL	1	Documnto sistema de gestión de seguridad de la información aprobado.	Implementación documental de SGSI (sistema de gestión de seguridad de la información ISO 27001:2022)	Documento del sistema de gestión de seguridad de la información elaborado y aprobado.	Ingeniero oficial de seguridad informática y protección de datos	0	1	0	

Fuente: Oficina asesora de planeación

- SEGUIMIENTO AL PLAN DE MANTENIMIENTO DE EQUIPOS DE CÓMPUTO, REDES Y SISTEMAS

El plan de mantenimiento de equipos de cómputo, redes y sistemas tiene como objetivo “Ejecutar mantenimiento preventivo anual, interno a los equipos de cómputo activos de la ESE ISABU con la finalidad de extender su vida útil, evitando daños futuros por el desgaste natural de los mismos”.

Para la vigencia 2023 el plan comprende la realización de 7 actividades con un total de 7 productos entregables de los cuales se observa con corte a 30 de junio de 2023 el cumplimiento del plan del 57% como se muestra a continuación:

PLAN	META ACTIVIDAD	INDICADOR META ACTIVIDAD	ACTIVIDAD DE TRABAJO	PRODUCTO / ENTREGABLE	RESPONSABLE	META EJECUTADA	META /ACTIVIDAD PROGRAMADA	RESULTADO META	CUMPLMIENTO DEL PLAN
PLAN DE MANTENIMIENTO DE EQUIPOS DE CÓMPUTO, REDES Y SISTEMAS	1	Plan e mantenimiento de equipos de cómputo, dispositivos de red y servidores	Elaborar el Plan de mantenimiento de equipos de cómputo, dispositivos de red y servidores para la vigencia 2023	Plan de mantenimiento de equipos de cómputo, dispositivos de red y servidores	Líder de Infraestructura Tecnológica	1	1	1	57%
PLAN DE MANTENIMIENTO DE EQUIPOS DE CÓMPUTO, REDES Y SISTEMAS	1	Un cronograma elaborado	Crear cronograma para los 3 mantenimientos preventivos programados por el PETI 2020-2023	Cronograma de mantenimiento preventivos programados para el periodo	Líder de Infraestructura Tecnológica	1	1	1	
PLAN DE MANTENIMIENTO DE EQUIPOS DE CÓMPUTO, REDES Y SISTEMAS	1	Link de publicación y socialización del plan de Mantenimiento de Equipos de Cómputo, dispositivos de red y Servidores	Publicar en página web institucional y socializar el plan de Mantenimiento de Equipos de Cómputo, dispositivos de red y Servidores por correo	Correo electrónico y link de página web institucional	Ing. de Seguridad Informática y Protección de Datos.	1	1	1	
PLAN DE MANTENIMIENTO DE EQUIPOS DE CÓMPUTO, REDES Y SISTEMAS	1	Informe presentado	Realizar mantenimiento preventivo # 1 de acuerdo al cronograma.	Informe de mantenimiento Preventivo # 1	Líder de Infraestructura Tecnológica	1	1	1	
PLAN DE MANTENIMIENTO DE EQUIPOS DE CÓMPUTO, REDES Y SISTEMAS	1	Informe presentado	Realizar mantenimiento preventivo # 2 de acuerdo al cronograma.	Informe de mantenimiento preventivo # 2	Líder de Infraestructura Tecnológica	0	1	0	
PLAN DE MANTENIMIENTO DE EQUIPOS DE CÓMPUTO, REDES Y SISTEMAS	1	Informe presentado	Realizar mantenimiento preventivo # 3 de acuerdo al cronograma.	Informe de mantenimiento preventivo # 3	Líder de Infraestructura Tecnológica	0	1	0	
PLAN DE MANTENIMIENTO DE EQUIPOS DE CÓMPUTO, REDES Y SISTEMAS	1	Informe presentado	Realizar mantenimiento preventivo de dispositivos de red y servidores.	Informe de mantenimiento anual de dispositivo de red y servidores	Líder de Infraestructura Tecnológica	0	1	0	

Fuente: Oficina asesora de planeación

<u>Observación</u>: De acuerdo con el seguimiento anterior, se puede indicar que en atención a los planes de acción MIPG correspondiente a las políticas de seguridad digital y gobierno digital formulados para la vigencia 2023, se evidenció el cumplimiento con lo programado a la fecha.

OPORTUNIDAD DE MEJORA: Pese a lo anterior, es necesario mencionar que para el cumplimiento del 100% del PETI, según la meta establecida, al término del cuatrienio (2020-2023), es prudente que las áreas involucradas, en lo relacionado con la renovación y adquisición de equipos tecnológicos, aúnen esfuerzos con el fin de acelerar los procesos contractuales de adquisición, teniendo en cuenta que a la vigencia le restan escasos cuatro (4) meses, que por las vicisitudes contractuales puedan poner en riesgo el cumplimiento del PETI, ya que las actividades incorporan no solo la adquisición de los equipos, sino la puesta en marcha de los mismos.

➢ <u>PLANES DE MEJORAMIENTO</u>

El proceso de Gestión de las TICS contaba con dos planes de mejoramiento:

- **Plan de mejoramiento vigencia 2022:** Cumplimiento al 100% de las metas programadas.

- **Plan de mejoramiento Vigencia 2021:** En el marco del Comité de Coordinación de Control Interno realizado el 14 de junio de 2023, la oficina de Planeación dio a conocer a los integrantes del Comité los inconvenientes para el cumplimiento de la metas pactadas, sumado a ello, expuso que la norma ISO sobre la cual se había realizado la auditoría cambió en la vigencia 2022; por lo anterior y con el fin de la mejora del proceso, el Comité de Coordinación de Control interno en pleno

aprobó la solución planteada por el área de Planeación y en la cual se describe un replanteamiento y ajuste a la nueva normatividad de las actividades para ser ejecutadas en la auditoría que ahora se desarrolla.

A continuación, se relacionan los hallazgos a los que deben replantearse las actividades del plan de mejoramiento:

No.	DESCRIPCIÓN DEL HALLAZGO
1	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
2	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.
3	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.
4	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.
5	En los contratos con personal y contratistas no se observan instrucciones en materia de manejo de reportes de debilidades y vulnerabilidades, incumpliendo de esta forma con lo establecido en el control A.16.1.2.
6	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

Estos hallazgos se trasladan como hallazgos aceptados por el auditado, haciéndose necesario modificar las actividades a realizar para cada uno de ellos, los cuales serán consignados en el plan de mejora producto de la presente auditoria. Es necesario aclarar que las actividades propuestas deben ser implementadas o ejecutadas en la vigencia 2023.

MAPA DE RIESGOS

Se evidenció en los mapas de riesgos de la E.S.E ISABU que el proceso Gestión de las TICS tiene identificado los siguientes riesgos para la vigencia 2023.

- MAPA DE RIESGOS DE CORRUPCIÓN-SICOF

Riesgo 11: “Posibilidad de afectación económica por sanciones impuestas por entidades de control por violación (modificación o eliminación) de datos personales debido a la combinación de amenazas y vulnerabilidades en el entorno digital a causa del incumplimiento en la actuación de licenciamientos y actualización de software contrafuegos”.

Riesgo 12: “Posibilidad de afectación económica por perdidas o daños en la infraestructura tecnológica (hardware, redes), debido al incumplimiento en procesos de controles o registro de inventarios a los equipos de cómputo y redes”.

- MAPA DE RIESGOS OPERACIONALES

- RIESGO OP 65: Posibilidad de pérdida económica, daños en la información que maneja la entidad, por un ataque cibernético y sanciones por pérdidas de los recursos financieros para el pago de obligaciones y funcionamiento de la entidad por ser vulnerables los sistemas de protección.

- RIESGO OP 66: Posibilidad de pérdida de confidencialidad, integridad y seguridad de los activos de información, por no ejecutar las actualizaciones de seguridad necesarias para la protección de atacante cibernéticos en los sistemas de información principal de la entidad.

- RIESGO OP 67: Posibilidad de pérdida de información y no disponibilidad de los servicios que presta la entidad debido a fallas en los PC y servidores por falta de mantenimiento, actualizaciones, reemplazo de elementos obsoletos y Ausencia de un esquema de contingencia.

- RIESGO OP 68: Posibilidad de afectación administrativa, disciplinaria por inadecuada aplicación de procedimientos desactualizados como el procedimiento de licenciamiento de equipos de cómputo y el procedimiento de soporte y mantenimiento de los servidores.

- RIESGO OP 69: Posibilidad de afectación administrativa y disciplinaria por falta de actualización del PETI y sus estrategias acordes a los riesgos identificados.

Observación:

La oficina de control interno ha venido realizando el seguimiento a los mapas de riesgos de Corrupción-SICOF y Operacionales del proceso Gestión TICS, evidenciándose la ejecución de controles; sin embargo, de la evaluación realizada se evidenció que nos encontramos ante un riesgo alto de materialización del riesgo operacional R. OP 65, al tener una vulnerabilidad por no contar con el licenciamiento del FIREWALL.

Igualmente, de la entrevista realizada con el área de las TICS se pudo identificar que los servidores comportan un riesgo extremo. Los servidores tienen una vida útil de 5 años y los que funcionan actualmente en la E.S.E ISABU reportan 10 años de uso, si un servidor presentara un daño no se cuenta con el debido soporte para la seguridad de la información, lo anterior genera alerta conforme a la priorización realizada en el riesgo (R.OP 67) "**Posibilidad de pérdida de información y no disponibilidad de los servicios que presta la entidad debido a fallas en los PC y servidores** por falta de mantenimiento, actualizaciones, reemplazo de elementos obsoletos y Ausencia de un esquema de contingencia.

OPORTUNIDAD DE MEJORA: En el riesgo operacional No. R. OP 68 correspondiente a "Posibilidad de afectación administrativa, disciplinaria por inadecuada aplicación de procedimientos desactualizados como el procedimiento de licenciamiento de equipos de cómputo y el procedimiento de soporte y mantenimiento de los servidores" se identifica la necesidad de actualizar estos dos procedimientos.

Teniendo en cuenta lo anterior y lo identificado en la auditoria, esta oficina de control interno determina la necesidad de **PRIORIZAR** la actualización de los procedimientos "licenciamiento de equipos de cómputo" y "soporte y mantenimiento de los servidores" a raíz que estos procedimientos

se encuentran relacionados con un riesgo operacional identificado.

Si bien en el plan de acción del mapa de riesgos, la fecha de implementación de las actividades se extiende hasta el 30 de noviembre de 2023, no es prudente esperar hasta tal fecha, ya que la identificación de la desactualización de los procedimientos genera que la probabilidad de la materialización del riesgo aumente.

REUNIÓN DE CIERRE

Se realizó reunión de cierre el día 17/08/2023 con la participación del Ing. William Figueroa Pineda profesional especializado del área de sistemas, Dr. Christian Camilo Rueda Sarmiento Subgerente Administrativo (e), Dra. Silvia Juliana Pinzón Cuevas jefe de control interno y los profesionales de apoyo de control interno Vianey González Gamarra y Elvis Jiménez Quiroz.

En la reunión de cierre, la jefe de control interno presenta los resultados y observaciones llevada a cabo a la Gestión de las TICS, expone los hechos que constituyen fortalezas y oportunidades de mejora, presenta un análisis de los riesgos relevantes dentro del proceso auditado.

Entendidos los resultados de la auditoría, el Ingeniero William Figueroa Pineda, en calidad de Líder del proceso TICS, **ACEPTA** el resultado del informe preliminar con los hallazgos y recomendaciones realizadas.

Ante la manifestación de aceptación realizada por el líder del proceso, la jefe de la oficina de control interno le informa que deberá entregar el respectivo plan de mejoramiento el cual deberá ser remitido a esta oficina de control interno en el término de diez (10) días hábiles.

Es necesario mencionar que la oficina de control interno recibe correo electrónico de fecha 17/08/2023 en el cual se confirma la aceptación de los hallazgos; por lo tanto, se determina el cierre de la auditoria al proceso de Gestión de las TICS.

PROCESO GESTIÓN DE LAS TICS				
CUADRO DE PRESUNTOS HALLAZGOS Y OPORTUNIDADES DE MEJORAMIENTO				
N°	**DESCRIPCIÓN**	**PH**	**OM**	**RG/ RC**
1.	En la auditoría realizada se procedió a verificar la aplicabilidad, vigencia y pertinencia de las actividades contenidas en los procedimientos, evidenciándose actualización de cuatro (4) procedimientos, a saber: Procedimiento Gestión de las tecnologías de la información, Procedimiento de identificación, gestión y clasificación de activos de información e infraestructura critica de TI, Procedimiento Gestión del Cambio y Procedimiento de Monitoreo y Seguimiento de Seguridad de la Información. Pese a lo antes señalado, algunos documentos de apoyo, manuales y procedimientos del área se encuentran desactualizados, como son: Procedimiento de licenciamiento de equipos de cómputo, Procedimiento de evaluación, soporte y mantenimiento preventivo y correctivo de Hardware, Procedimiento soporte y mantenimiento de servidores, procedimiento de solicitud de información, plan de contingencia informática, plan de contingencia ante no funcionamiento de historia clínica electrónica, política transparencia, acceso a la información pública y lucha contra la corrupción y la política de la seguridad de la información (2017).	X		
2	En la revisión realizada se detectó que en el listado maestro de documentos de gestión de las TICS se relacionan procedimientos que no pertenecen al área. Por lo tanto, es necesario que las TICS realice junto a la oficina de Calidad, una actualización y depuración del listado maestro de documentos.		X	
3	Al aplicar los procedimientos de evaluación, soporte y mantenimiento preventivo y correctivo de hardware y el procedimiento de soporte y mantenimiento de servidores en la visita realizada a la Gestión de las TICS, esta oficina de control interno evidenció que no se cuenta con un archivo físico o electrónico (hoja de vida), en donde se lleve control efectivo y consolidado por equipos de cómputo y servidores, que brinde información relevante como: información del usuario (nombre del usuario, cargo, área y responsable del equipo), información de adquisición (tiempo de garantía, entidad o proveedor, fabricante), información del equipo (tipo, modelo, marca y serie, numero de inventario, IP, monitor, hardware, entre otros). Lo anterior es de vital importancia con el fin que cada equipo de cómputo y servidor cuente con un registro, memoria y trazabilidad histórica que le permita a las TICS la toma de decisiones acertadas respecto a bajas, mantenimientos o adquisiciones.	X		

PROCESO GESTIÓN DE LAS TICS				
CUADRO DE PRESUNTOS HALLAZGOS Y OPORTUNIDADES DE MEJORAMIENTO				
N°	**DESCRIPCIÓN**	**PH**	**OM**	**RG/ RC**
4.	Pese a lo anterior, es necesario mencionar que para el cumplimiento del 100% del PETI, según la meta establecida, al término del cuatrienio (2020-2023), es prudente que las áreas involucradas, en lo relacionado con la renovación y adquisición de equipos tecnológicos, aúnen esfuerzos con el fin de acelerar los procesos contractuales de adquisición, teniendo en cuenta que a la vigencia le restan escasos cuatro (4) meses, que por las vicisitudes contractuales puedan poner en riesgo el cumplimiento del PETI, ya que las actividades incorporan no solo la adquisición de los equipos, sino la puesta en marcha de los mismos.		X	
5.	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	X		
6.	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.	X		
7.	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.	X		
8.	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	X		
9.	En los contratos con personal y contratistas no se observan instrucciones en materia de manejo de reportes de debilidades y vulnerabilidades, incumpliendo de esta forma con lo establecido en el control A.16.1.2.	X		
10.	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	X		

PROCESO GESTIÓN DE LAS TICS				
CUADRO DE PRESUNTOS HALLAZGOS Y OPORTUNIDADES DE MEJORAMIENTO				
N°	**DESCRIPCIÓN**	**PH**	**OM**	**RG/ RC**
	establecido en el control A.17.1.1			
11.	En el riesgo operacional No. R. OP 68 correspondiente a "Posibilidad de afectación administrativa, disciplinaria por inadecuada aplicación de procedimientos desactualizados como el procedimiento de licenciamiento de equipos de cómputo y el procedimiento de soporte y mantenimiento de los servidores" se identifica la necesidad de actualizar estos dos procedimientos. Teniendo en cuenta lo anterior y lo identificado en la auditoria, esta oficina de control interno determina la necesidad de PRIORIZAR la actualización de los procedimientos "licenciamiento de equipos de cómputo" y "soporte y mantenimiento de los servidores" a raíz que estos procedimientos se encuentran relacionados con un riesgo operacional identificado. Si bien en el plan de acción del mapa de riesgos, la fecha de implementación de las actividades se extiende hasta el 30 de noviembre de 2023, no es prudente esperar hasta tal fecha, ya que la identificación de la desactualización de los procedimientos genera que la probabilidad de la materialización del riesgo aumente.		X	

PH: PRESUNTO HALLAZGO
OM: OPORTUNIDAD DE MEJORA
RG/RC: RIESGO DE GESTIÓN/RIESGO DE CORRUPCION

RECOMENDACIONES

- En el marco del mejoramiento continuo, se recomienda continuar con el fortalecimiento del recurso humano y de infraestructura tecnológica con el fin de dar cumplimiento a todas las tareas específicas de Gestión de las TICS.
- A lo largo del texto de la presente auditoria, se relacionan recomendaciones que, si bien no generan una actividad ligada a un hallazgo, es preciso que las Gestión de las TICS las tenga en cuenta para su implementación em pro del mejoramiento continuo.

FORTALEZAS

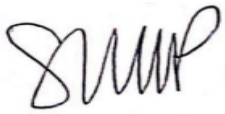
- Se destaca el compromiso y la disposición del personal del área de Gestión de las TIC en el desarrollo de la auditoria.

- Se observa la mejora continua, mediante la actualización que se está llevando de los documentos que hacen parte del proceso.

CONCLUSIONES

- En el marco del mejoramiento continuo, se recomienda continuar con el fortalecimiento del recurso humano y de infraestructura tecnológica con el fin de dar cumplimiento a todas las tareas específicas de Gestión de las TICS.
- A lo largo del texto de la presente auditoria, se relacionan recomendaciones que, si bien no generan una actividad ligada a un hallazgo, es preciso que las Gestión de las TICS las tenga en cuenta para su implementación en pro del mejoramiento continuo.

Equipo auditor,



SILVIA JULIANA PINZÓN CUEVAS
Jefe Oficina de Control Interno

Equipo auditor de apoyo:

Vianey González Gamarra – Elvis Jiménez Quiroz
Profesionales de apoyo Oficina de control interno