1300-39.01
CI-191

Firma_____
Radicado: **00004360**
Enviado: 16/12/2021 - 2:51 p.m.
abenitez
ESE ISABU

Bucaramanga, 16 de diciembre de 2021

Señores
E.S.E. ISABU
Dr. GERMAN JESUS GOMEZ LIZARAZO
Gerente
Dr. ELVIS JIMÉNEZ QUIROZ
Jefe Oficina Asesora de Planeación (E)
Ing. CARLOS ANDRÉS SIERRA CARVAJAL
Profesional especializado – Planeación. Apoyo Gestión TIC´s

Asunto: informe final auditoria de las TIC´s de la ESE ISABU.

Cordial saludo:

La Oficina de Gestión y Control Interno de la E.S.E. ISABU, en desarrollo de sus funciones y conforme al plan de auditoria basados en riesgos para la vigencia 2021, presenta informe final de la auditoria de las TIC´s.

Agradezco su atención.

Cordialmente,

CIRO ELBERTO GAMBOA SERRANO
Jefe Oficina de Gestión y Control Interno

P/E: William Figueroa Pineda
Profesional de apoyo control interno

Revisó: Ciro Elberto Gamboa Serrano
Jefe Oficina de Gestión y Control Interno

AUDITORIA DE PROCESO Y/O SUBPROCESO:

GESTION TIC

FECHA:

16 de diciembre de 2021

RESPONSABLES DEL PROCESO:

Doctor Elvis Jiménez Quiroz
Jefe Oficina Asesora de Planeación (E)
Ingeniero Carlos Andrés Sierra Carvajal
Profesional especializado – Planeación. Apoyo Gestión TIC´s

ALCANCE:

- Verificar y evaluar las actividades del proceso gestión de las TIC de la E.S.E ISABU, a fin de establecer oportunidades de mejora que contribuyan a la adecuada gestión del mismo.

OBJETIVOS:

- Evaluar y verificar el proceso gestión de las TICS de la E.S.E ISABU, en cumplimiento de procedimientos y demás actividades.

- Dar cumplimiento con en el Programa de Auditorías basadas en riesgos de la vigencia 2021.

MARCO NORMATIVO:

- 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 informaci6n y la organizaci6n 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 la Estrategia de Gobierno en Línea.

- *Documento CONPES 3785 DEL 9 de Diciembre de 2013. Describe la política nacional de servicio al ciudadano.*

- *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."

VISITAS Y ENTREVISTAS REALIZADAS:

Para el desarrollo de la presente auditoria se aplicaron técnicas verbales y escrita, y se solicitó información y análisis documental, a los siguientes funcionarios:

- Ingeniero Carlos Andrés Sierra Carvajal.
- Ingeniera Leidy Viviana Córdoba Flórez
- Ingeniero Rubén Darío Lozano Ortega.
- Doctor Elvis Jiménez Quiroz.
- Doctora Clara Inés Strauch Díaz.

ACEPTACION O NO ACEPTACIÓN DEL HALLAZGO:

La oficina de Gestión y Control Interno de la E.S.E. ISABU, en cumplimiento de sus funciones y al Plan General de Auditoría de la vigencia 2021 y en el marco del MIPG, presenta informe final de auditoría realizado al proceso Gestión de las TICs.

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

Los hallazgos encontrados y aceptados por la Gestión de las TICs con la recomendación de Control Interno, son los siguientes:

Hallazgo 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.

Aceptación hallazgo 1: se acepta hallazgo y se plantea plan de mejora para la vigencia del 2022 segundo trimestre siempre y cuando la administración nos apoye con la contratación del profesional oficial de protección de Datos.

Recomendación 1: para lograr la mejora continua tal como lo señala la Ley de Protección de Datos Personales, se debe hacer énfasis en el Sistema de Gestión de Seguridad de la Información (SGSI).

La política de seguridad de la información debería contener declaraciones relativas a:

- La definición de la seguridad de la información, de sus objetivos y principios, para orientar todas las actividades concernientes a la seguridad de la información.
- La asignación de responsabilidades generales y específicas en materia de gestión de la seguridad de la información, para los roles definidos.

- La política de seguridad de la información debería apoyarse en políticas sobre temas específicos que profundicen en la implantación de controles y que, por lo general, estén estructuradas para atender las necesidades de determinados grupos dentro de una organización o para cubrir ciertos temas como:

  - Política Control de Acceso.
  - Plan de sensibilización, comunicación
  - Clasificación de la información.
  - Seguridad física y ambiental.
  - Uso adecuado de activos.
  - Puesto de trabajo despejado y pantalla limpia.
  - Transferencia de información.
  - Dispositivos móviles y teletrabajo.
  - Restricciones de instalación y uso de software.
  - Política de Backup.
  - Protección ante el software malicioso.
  - Gestión de vulnerabilidades técnicas.
  - Seguridad de las comunicaciones.
  - Privacidad y protección de la información identificativa de personas.
  - Relaciones con proveedores.

- Cada política debería tener un propietario a quien la Dirección le ha asignado la responsabilidad de su desarrollo, revisión y evaluación. La revisión debería incluir la evaluación de oportunidades de mejora de las políticas de seguridad y un enfoque de cómo gestionar la seguridad de la información en respuesta a los cambios del entorno de la organización, de las circunstancias del negocio, de las condiciones legales reglamentarias o contractuales o del entorno técnico.

Hallazgo 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.

Aceptación hallazgo 5: Este Hallazgo se plantea mejora con la Actualización propuesta en el Hallazgo 1.

Recomendación 5: para lograr la mejora continua tal como lo señala la Ley de Protección de Datos Personales, se debe hacer énfasis en el Sistema de Gestión de Seguridad de la Información (SGSI).

Hallazgo 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.

Aceptación hallazgo 8: Se acepta el Hallazgo, Actualmente se está adelantado un proceso entre las dependencias de Almacén – Costos – Contabilidad y Sistemas para que, en el mes de diciembre del 2021, se suba la cantidad total de activos fijos por archivo plano generando los movimientos de Entrada y Hoja de vida, A su vez la depreciación contable.

Recomendación 8: La información y otros activos asociados a la información y a los recursos para el tratamiento de la información deberían estar claramente identificados y debería elaborarse y mantenerse un inventario.

- La organización debería identificar los activos relevantes para el ciclo de vida de la información y documentar su importancia. El ciclo de vida de la información debería incluir la creación, tratamiento, almacenamiento, transmisión, borrado y destrucción. La documentación debería ser mantenida en inventarios dedicados o existentes según lo que sea adecuado.

  - Inventario de Activos: Software.
  - Propiedad de los activos: Todos los activos que figuran en el inventario deberían tener un propietario.
  - Uso aceptable de los activos: Se deben identificar, documentar e implementar las reglas de uso aceptable de la información y de los activos asociados con los recursos para el tratamiento de la información.
  - Devolución de activos. Todos los funcionarios o contratistas deberán devolver todos activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo.
  - Clasificación de la información.

- Se aclara que el inventario que se está llevando actualmente está correcto, pero en este punto se hace referencia a los Activos de Información que por norma requieren un trato diferente.

Hallazgo 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.

Aceptación hallazgo 9: Se acepta Hallazgo y se plantea plan de mejora para la vigencia 2022 segundo trimestre.

Recomendación 9: Se deberían implementar procedimientos para la gestión de los soportes extraíbles, de acuerdo con la clasificación adoptado por la organización.

Deberían considerarse las directrices siguientes para la gestión de soportes extraíbles:

- En caso de ya no ser necesarios, deberían borrarse definitivamente los contenidos de cualquier soporte reutilizable que vaya a ser retirado.

- Cuando sea necesario y práctico, debería solicitarse autorización para extraer soportes de la organización, y debería mantenerse un registro de tales retiradas para mantener la trazabilidad a efectos de auditoría.

- Deberían emplearse técnicas criptográficas para proteger datos en soportes extraíbles en caso de que apliquen requisitos importantes de confidencialidad o integridad.

- Deberían almacenarse copias múltiples de datos valiosos en soportes separados para reducir aún más el riesgo de daño o pérdida simultánea de los datos.

- Solo deberían permitirse reproductores de soportes extraíbles cuando haya una razón de negocio para ello.

Hallazgo 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.

Aceptación hallazgo 14: Se acepta Hallazgo, y se plantea mejora a la administración según la asignación de recursos para la vigencia del 2022.

Recomendación 14: Los equipos deberían situarse o protegerse de forma que se reduzcan los riesgos de las amenazas y los riesgos ambientales así como las oportunidades de que se produzcan accesos no autorizados.

- Se deberían adoptar controles para minimizar el riesgo de posibles amenazas físicas y ambientales como, por ejemplo, robo, fuego, explosivos, humo, agua, polvo, vibración, agentes químicos, interferencias en el suministro eléctrico, interferencias en las comunicaciones, radiaciones electromagnéticas y vandalismo;

- Se deberían controlar las condiciones ambientales, tales como la temperatura y la humedad (aire acondicionado), que puedan afectar negativamente al funcionamiento de los equipos de tratamiento de información.

- Se deberían aplicar sistemas de protección contra rayos en todos los edificios y colocar filtros de protección contra rayos en todas las entradas de corriente eléctrica y en todas las líneas de comunicación;

- Se debería adoptar la red regulada para proteger los diferentes dispositivos de cómputo.

- Los suministros de apoyo como, por ejemplo, electricidad, telecomunicaciones, agua, gas, aguas residuales, calefacción/ventilación y aire acondicionado, deberían:

  - Ser conformes a las especificaciones del fabricante de los equipos y a los requisitos legales locales.

  - Ser evaluadas regularmente respecto a su capacidad para satisfacer el desarrollo de negocio y respecto a la interacción con otros servicios de apoyo.

  - Ser inspeccionadas regularmente mediante las pruebas apropiadas para asegurar su correcto funcionamiento.

  - En caso necesario, disponer de alarmas para detectar fallos en su funcionamiento.

  - En caso necesario, disponer de múltiples fuentes con canales físicos de alimentación independientes.

- Debería proporcionarse alumbrado y comunicaciones de emergencia. Los interruptores y válvulas de emergencia para cortar el suministro de energía, agua, gas u otros servicios no deberían estar ubicados cerca de las salidas de emergencia o de las salas de los equipos.

- Se puede conseguir redundancia adicional para la conectividad de las redes por medio de múltiples rutas aportadas por más de un proveedor de servicios.

Hallazgo 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.

Aceptación hallazgo 15: se acepta el Hallazgo, se plantea plan de mejora para la vigencia del primer semestre del 2022

Recomendación 15: El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información debería estar protegido frente a interceptaciones, interferencias o daños.

- Se deberían considerar las siguientes directrices para la seguridad del cableado.
- Las líneas de energía y telecomunicaciones en las zonas de tratamiento de información, deberían ser debajo de la superficie, cuando sea posible, o adoptarse medidas alternativas de protección.
- Se deberían separar los cables de energía de los de comunicaciones para evitar interferencias.

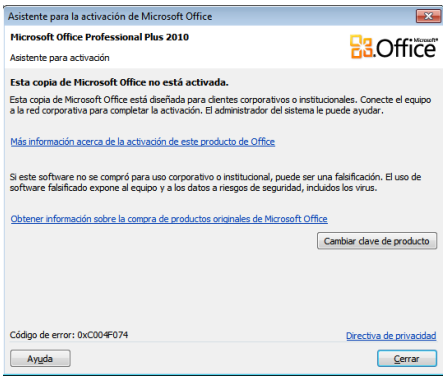
Hallazgo 18: No se evidencia un seguimiento al control de cambios, incumpliendo de esta forma con lo establecido en el control A.12.1.2 de la Norma ISO 27001:2013.

Aceptación hallazgo 18: Se acepta Hallazgo, y se plantea mejora para la vigencia del 2022.

Recomendación 18: Se deberían considerar los siguientes puntos:

- La identificación y registro de los cambios significativos.
- La planificación y pruebas de los cambios.
- La evaluación de los impactos potenciales, incluyendo los impactos en la seguridad de la información de dichos cambios.
- El procedimiento de aprobación formal de los cambios propuestos.
- La verificación de que los requisitos de seguridad de la información se cumplen.
- La comunicación de los detalles de los cambios a todas las personas correspondientes.
- Los procedimientos de vuelta atrás, incluyendo los procedimientos y responsabilidades para abortar y recuperar los cambios infructuosos y los eventos imprevistos.
- La disposición de un proceso de cambio de emergencia que habilite la implantación rápida y controlada de los cambios necesarios para resolver un incidente.

Hallazgo 24: Se evidencia la falta de licenciamiento de software Microsoft office en algunos equipos.



Aceptación hallazgo 24: Se acepta Hallazgo, y se plantea mejora a la administración según la asignación de recursos para la vigencia del 2022.

Recomendación 24: Actualización del licenciamiento del software Microsoft office ya el uso de este sin licencia conlleva a sanciones legales y fiscales.

Los hallazgos 12 y 13 no serán tenidos en cuenta en el informe final de la presente auditoria, en razón a que en reunión con Ingeniero Carlos Andrés Sierra Carvajal y el profesional de Apoyo de Control Interno William Figueroa Pineda se puedo establecer que los determinado en dichos hallazgos, no aplican al proceso auditado.

RESPUESTA OFICINA DE CONTROL INTERNO

La oficina de control interno, en cumplimiento de sus funciones y siguiendo los lineamientos establecidos por el Departamento Administrativo de la Función Pública DAFP, en la guía de auditoria interna basada en riesgos para entidades públicas Versión 4, y habiéndose dado los términos para responder, lo planteado por la oficina de Control Interno, se encuentra que **NO SE ACEPTAN los** hallazgos que se relacionan.

1. Hallazgo 2
2. Hallazgo 3
3. Hallazgo 4
4. Hallazgo 6
5. Hallazgo 7
6. Hallazgo 10
7. Hallazgo 11
8. Hallazgo 16
9. Hallazgo 17
10. Hallazgo 19
11. Hallazgo 20
12. Hallazgo 21
13. Hallazgo 22
14. Hallazgo 23
15. Hallazgo 25

En procura del mejoramiento continuo de la entidad y siendo la debida utilización de los recursos tecnológicos un instrumento fundamental para el cumplimiento de la misión de la ESE ISABU, la oficina de Control Interno ratifica los hallazgos ya señalados y para los cuales se deben plantear los respectivos planes de mejora.

La oficina de control interno, realizará los respectivos seguimientos, para verificar que las acciones previstas en los planes de mejoramiento sean implementadas, para de esta forma superar positivamente los hallazgos y así lograr el cumplimiento de la misión institucional y el manejo eficiente y eficaz de los recursos.

PLANES DE MEJORAMIENTO

- La Implementación del Sistema de Gestión de Seguridad de la Información, que deben ser propuestos en los respectivos planes de mejora, deben estar acordes con lo aprobado en plan de desarrollo en la ESE Instituto de Salud de Bucaramanga 2020 – 2023, donde se plantea el uso óptimo y eficiente de los recursos físico y tecnológicos, que agreguen valor a los servicios institucionales, y cumpliendo con los estándares de infraestructura, seguridad y habilitación de todos los servicios.

RECOMENDACIONES

- Para optimizar los recursos y brindar un mejor servicio a los usuarios, se recomienda el desarrollo de implementación del Sistema de Gestión de Seguridad de la Información.
- Preserva la confidencialidad, la integridad y la disponibilidad de la información, mediante la aplicación de un proceso de gestión del riesgo, y brindar confianza a la ESE ISABU acerca de los riesgos gestionados.
- Identificación de los activos de información.
- Identificación, análisis, evaluación y tratamiento de los riegos de los activos de información.
- Se recomienda frente a la contingencia COVID-19, mantener la integridad de la información de la ESS ISABU y poner en marcha estrategias para evitar ataques cibernéticos, recordar a los colaboradores las políticas de seguridad de la información y el uso y privacidad de los datos, así mismo proteger y monitorear los sistemas de información a través de Backus, antivirus que cubra todos los dispositivos que acceden a la información de la entidad, firewall, entre otros, con el objetivo de mitigar el riesgo de pérdida, indisponibilidad, deterioro o acceso no autorizado.
- Tener en cuenta las recomendaciones presentadas en el informe para la implementación del SGSI.

CONCLUSIONES

- Como aspectos positivos encontramos:
  - Un gran número de usuarios, que felicitan a la Oficina de las TICs en el soporte que brinda en la entidad, viendo el gran esfuerzo que realizan para ello.
  - El esfuerzo para implementar una sólida infraestructura informática y tratar de mantenerla actualizada, data center, redes, etc.
  - La recursividad en la búsqueda de alternativas a cada una de las necesidades que se presentan, que en ocasiones sin contar con los recursos idóneos.
- Cabe recalcar y lo importante que fue la socialización de la Ley de Protección de Datos, y es necesario continuar trabajando en la Ley de Protección de Datos Personales e implementar el SGSI con el fin de mejorar el índice de evaluación.
- Se reitera el fortalecimiento de la infraestructura tecnológica de la ESE ISABU.
- Se encuentran en desarrollo la implementación de la Ley de Protección de Datos Personales.

- Se debe mantener, y fortalecer a través de acciones de mejora continua y así facilitando anticipar y corregir de manera oportuna las debilidades que se presentan en el desarrollo de las actividades de los procesos de la ESE ISABU, mitigando la materialización de riesgos asociados.
- La presente auditoria se finalizó cumpliendo con los principios éticos, brindando la oportunidad de contradicción, y siempre en procura del mejoramiento continuo de la entidad.

Equipo auditor,

CIRO ELBERTO GAMBOA SERRANO
Jefe Oficina de Gestión y Control Interno

WILLIAM FIGUEROA PINEDA
Profesional de apoyo control interno

P/E: William Figueroa Pineda
Profesional de apoyo control interno
Revisó: Ciro Elberto Gamboa Serrano
Jefe Oficina de Gestión y Control Interno