INSTITUTO DE PLANIFICACION Y PROMOCION DE SOLUCIONES ENERGETICAS PARA LAS ZONAS NO INTERCONECTADAS – IPSE

GRUPO CONTROL INTERNO

INFORME FINAL

AUDITORÍA INTERNA A LOS PROCESOS DE LAS TECNOLOGÍAS DE LA INFORMACIÓNY COMUNICACIONES – TIC IPSE 2021

BOGOTÁ, DICIEMBRE 2021

TABLA DE CONTENIDO

6.1.3. Sistema contra incendios sin registro de mantenimiento ni recarga en el centro de datos.
6.1.4. Riesgo de desconexión eléctrica y corto circuito en el centro de datos.
6.1.5. Riesgo de desconexión de red de datos de los equipos en el centro de datos.
6.1.6. Riesgo de desconexión de red del equipo FortiAnalizer del sistema de seguridad Firewall del centro de datos.
6.1.7. No se evidencio el diagrama de arquitectura de red de la infraestructura tecnológica del centro de datos.

6.2 Centro de datos IPSE CNM – Infraestructura Tecnológica

- Descripción de la visita
- Observaciones al centro de datos IPSE CNM

6.2.1. Falla de seguridad de control de acceso al centro de datos.
6.2.2. Falta de mantenimiento de la UPS del centro de datos.
6.2.3. Se observa que el centro de datos no tiene un sistema contra incendios tipo fijo, de operación automática, propio de un centro de datos.
6.2.4. Falla del aire acondicionado del centro de datos.
6.2.5. Alto nivel de contaminación por polvo en los servidores, equipos de comunicación y equipos de seguridad del centro de datos.
6.2.6. Riesgo de desconexión eléctrica y corto circuito en el centro de datos.
6.2.7. Riesgo de desconexión de red de datos de los equipos en el centro de datos.

6.3 Centro de datos IPSE SOACHA – Infraestructura Tecnológica

- Descripción de la visita
- Observaciones al centro de datos IPSE SOACHA

6.3.1. Falla en la acometida eléctrica de red normal al centro de datos.
6.3.2. Falla en el sistema de puesta a tierra que ingresa al tablero eléctrico del centro de datos.
6.3.3. No existe sistema de pararrayos en el edificio del centro de datos.
6.3.4. La infraestructura de red eléctrica del centro de datos presenta riesgo de corto circuito e incendio.
6.3.5. Almacenamiento irregular de combustible en el centro de datos, incumpliendo la norma NTC 2885 de 2009.
6.3.6. Falla en el sistema de trasferencia automática de energía del centro de datos.
6.3.7. Falla de seguridad de control de acceso al centro de datos.
6.3.8. No se evidencia que el sistema de video seguridad este en funcionamiento en el centro de datos.
6.3.9. El rack de comunicaciones del centro de datos no tiene una organización técnica de cableados de energía y comunicaciones.
6.3.10 Alto nivel de contaminación por polvo en los servidores, equipos de comunicación y equipos de seguridad del centro de datos.
6.3.11. El centro de datos del CNM no está integrado al centro de datos alterno de SOACHA.

6.4 Plan Estratégico de Tecnológicas de la Información - PETI

- Descripción del contexto PETI IPSE
- Observaciones al Plan Estratégico de Tecnológicas de la Información - PETI

6.4.1. El IPSE no tiene en funcionamiento una herramienta software de Arquitectura Empresarial AE.

6.4.2. Los documentos técnicos del capítulo “SITUACION ACTUAL” del PETI IPSE 2020-2023, están desactualizados y no reflejan la situación actual AS-IS del IPSE.

6.4.3. En el documento PETI IPSE 2020-2023 no está el capítulo de SITUACIÓN OBJETIVO TO-BE, el cual hace parte fundamental de la estructura de un Plan Estratégico de Tecnologías de la Información de una entidad.

6.4.4. En el capítulo de “*Identificación de Hallazgos y Brechas”*, del documento PETI IPSE 2020-2023, no se tiene un identificador ID por cada brecha, por tanto, no es posible identificar en el portafolio de proyectos, que brechas se cierran con cada proyecto del mapa de ruta.

6.4.5. El documento PETI 2020-2023 indica cuatro listados de proyectos TI, que no están alienados entre ellos.

6.5 Política de Seguridad y Privacidad de la Información.

6.5.1. El documento de *“Políticas de Seguridad y Privacidad de la Información del IPSE*” esta desactualizado.

6.6 Procedimiento de BACKUPS de Información.

6.6.1. El procedimiento de backups registrado en el Sistema de Gestión Integral - SGI código IPSE-TIC-P04 esta desactualizado.

6.7 Seguimiento a los radicados del sistema de información ORFEO sin digitalizar en el periodo de enero a julio 2021.

6.7.1. Radicados de ORFEO sin digitalizar.

6.8. SEGUIMIENTO AL SISTEMA DE INFORMACIÓN SGI – SISTEMA GESTION INTEGRAL

6.8.1. El Sistema Gestión Integral SGI del IPSE, no está operativo.

7. RESULTADOS DE LA ENCUESTA DE PERCEPCIÓN TI IPSE 2021

8. CONCLUSIONES

INFORME PRELIMINAR DE AUDITORÍA INTERNA A LOS PROCESOS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES – TIC IPSE 2021

1. PROCESO A AUDITAR

Auditoría al proceso de Gestión de Tecnologías de la Información y Comunicaciones TICs y su soporte con los sistemas y procesos internos de la Entidad.

Fuente Sistema de Gestión Integral – SGI. Proceso Gestión de TICs

IPSE-TIC-C01 Caracterización del proceso de Gestión de TICs

Objetivo: Gestionar estratégicamente las necesidades de innovación en tecnología, seguridad y operatividad que requieran las partes interesadas, con el fin de apoyar el cumplimiento de los objetivos institucionales en el marco de la estrategia de Gobierno Digital.

Los procedimientos del proceso de Gestión TICs son:

IPSE-TIC-P02 Procedimiento seguridad y privacidad de la información.

Objetivo: Proteger los activos de información del IPSE soportados por los servicios de TI, enfocándose en la confidencialidad, integridad y la continuidad de los mismos.

- Administración, identidad y cuentas de usuario.
- Backup's de información y transferencia.
- Protección software y hardware.

IPSE-TIC-P03 Procedimiento de innovación tecnológica.

Objetivo: Gestionaren el IPSE con eficiencia (gestión de los recursos) y eficacia (consecución de los objetivos) las capacidades tecnológicas de una manera continua, permitiendo al Proceso de Gestión de TIC innovar y mejorar las diferentes estrategias para atender los requerimientos de las partes interesadas tomando como referencia el mercado.

IPSE-TIC-P04 Procedimiento de soporte y mantenimiento hardware y software.

Objetivo: Soportar y mantener el hardware y software del IPSE

2. OBJETIVOS DE AUDITORIA

2.1 OBJETIVO GENERAL

Realizar auditoria a las actividades tecnológicas de la información del IPSE, teniendo en cuenta los siguientes aspectos:

- Planeación Estratégica y Operativa
- Procedimientos registrados en el Manual del Sistema de Gestión Integral
- Servicios que presta el Grupo de TIC´s
- Análisis de la infraestructura Tecnológica de la entidad
- Análisis de administración de riesgos
- Análisis de la continuidad del negocio
- Análisis y seguimiento a las recomendaciones de auditoría TIC´s 2017

2.2 OBJETIVOS ESPECIFICOS

- Compilar la información de interés de la auditoria, para analizar la evolución del manejo de la Coordinación de Tecnologías y Sistemas de la Información en las últimas vigencias.
- Realizar seguimiento a las observaciones de auditoría IPSE TI 2017.
- Evaluar la interacción entre la infraestructura tecnológica, sistemas de información y procesos del IPSE.
- Realizar seguimiento al Plan Estratégico de Tecnología PETIC del IPSE.
- Realizar seguimiento a las inversiones relacionadas con Tecnologías de la Información y Comunicaciones del IPSE en el periodo de 2017 a 2021, en cuyo desarrollo se podrá seleccionar una muestra para su análisis.
- Realizar una encuesta de percepción actual de los clientes internos del IPSE frente a la plataforma tecnológica, en relación a las actividades de cada proceso de la entidad y a las nuevas condiciones de trabajo desde casa.
- Realizar análisis de seguridad de la plataforma tecnológica identificando los riesgos y sus controles para mitigarlos.

3. ALCANCE DE AUDITORIA

Se propone utilizar la estructura de seis (6) componentes con sus líneas de acción de acuerdo con el modelo IT4+ propuesto por MINTIC, para incorporar todas las iniciativas relacionadas con la gestión de TI de la organización.

La siguiente Tabla detalla la estructura que incorpora todas las iniciativas relacionadas con la gestión de TI de la organización para hacer el seguimiento, de acuerdo con las Líneas de acción por componente de IT4+[2]:

Componente	Líneas de acción
1. Planear, definir y mantener la estrategia de TI	1.1 Alineación de iniciativas con la estrategia institucional o sectorial 1.2. Plan de seguridad 1.3. Plan de continuidad de TI 1.4. Fortalecimiento de la gestión Integral de TI
2. Planear, definir y mantener el gobierno de TI	2.1. Fortalecimiento de la estructura organizacional de TI 2.2. Marco de gobernabilidad de TI 2.3. Definición e implantación de procesos de gestión de TI
3. Análisis de Información	3.1. Desarrollo de la arquitectura de información 3.2. Desarrollo de la capacidad de consolidación y publicación de informació 3.3. Desarrollo de la capacidad de análisis de información
4. Desarrollar y mantener los Sistemas de Información	4.1. Desarrollo y consolidación de los sistemas de información de apoyo administrativo 4.2. Desarrollo y consolidación de los sistemas de información misionales 4.3 Desarrollo y consolidación de los servicios informativos digitales 4.4. Desarrollo y consolidación de los sistemas de direccionamiento
5. Gestionar Servicios Tecnológicos	5.1. Infraestructura de datacenter 5.2. Hardware y software de oficina 5.3. Licenciamiento de software de datacenter 5.4. Conectividad 5.5. Servicios de operación (administración de infraestructura, DBA, consultorías, tercerización, etc) 5.6. Servicios informáticos (correo electrónico, directorio activo, antivirus, proxies, mensajería, impresión, etc) 5.7. Servicios en la nube (IAAS, PAAS) 5.8. Servicio de soporte y mesa de ayuda 5.9. UPS y sistema eléctrico 5.10. Servicios de telefonía 5.11. Servicios de seguridad electrónica y video-vigilancia
6. Uso y apropiación de TI	6.1. Capacitación 6.2. Herramientas para el aprendizaje 6.3. Planes de implantación 6.4. Evaluación del nivel de adopción de tecnología y satisfacción en el uso.

Líneas de acción por componente de IT4+[3]

4. NORMATIVIDAD

4.1. MANUAL DE GOBIERNO DIGITAL

El Manual de Gobierno Digital es el documento que establece los lineamientos y estándares de los componentes de la política (TIC para el Estado y TIC para la Sociedad) y de los habilitadores transversales (arquitectura, seguridad y privacidad de la información y

servicios ciudadanos digitales).

"Implementar - ¿Cómo iniciar la ejecución?
*Una vez la entidad cuente con el **PETI** y el **plan de seguridad y privacidad de la información**, en donde se definieron los proyectos y se establecieron las actividades, responsables, tiempos de ejecución y recursos para la ejecución de la política, ésta debe desarrollar dichas iniciativas o proyectos, aplicando lineamientos que corresponden a los componentes TIC para el Estado y TIC para la Sociedad..."*

*"...se entiende por **lineamiento** la directriz o disposición establecida por el Ministerio TIC, que debe ser implementada por las entidades públicas para el desarrollo de la política de Gobierno Digital y se desarrolla a través de estándares, guías, recomendaciones o buenas prácticas..."*

Fuente:
https://gobiernodigital.mintic.gov.co/portal/Politica-de-Gobierno-Digital/Manual-de-Gobierno-Digital/

4.2. RESOLUCIÓN 00500 DE MARZO 10 DE 2021

"Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad con habilitador de la política de Gobierno Digital"

Fuente:
https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf

4.3. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - MSPI

El Modelo de Seguridad y Privacidad de la Información - MSPI, imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital.

Para que las entidades públicas incorporen la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y, en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

Sé encuentra alineado con el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y La Guía para la Administración del Riesgo y el Diseño

Controles en entidades Públicas, este modelo pertenece al habilitador transversal de Seguridad y Privacidad, de la Política de Gobierno Digital.

Y se desarrolla mediante el Documento Maestro del Modelo de Seguridad y Privacidad de la Información y sus guías de orientación. Lo debe desarrollar el líder o encargado de Seguridad de la Información con el apoyo de toda la estructura organizacional.

Modelo de Seguridad y Privacidad - MSPI
Guía 1 - Metodología de pruebas de efectividad
Guía 2 - Política General MSPI v1
Guía 3 - Procedimiento de Seguridad de la Información
Guía 4 - Roles y responsabilidades
Guía 5 - Gestión Clasificación de Activos
Guía 6 - Gestión Documental
Guía 7 - Gestión de Riesgos
Guía 8 - Controles de Seguridad de la Información
Guía 9 - Indicadores Gestión de Seguridad de la Información
Guía 10 - Continuidad de Negocio
Guía 11 - Análisis de Impacto de Negocio
Guía 12 - Seguridad en la Nube
Guía 13 - Evidencia Digital
Guía 14 - Plan de comunicación, sensibilización, capacitación
Guía 15 - Auditoria
Guía 16 - Evaluación de Desempeño
Guía 17 - Mejora continua
Guía 18 - Lineamientos terminales de áreas financieras de entidades públicas
Guía 19 - Aseguramiento de protocolo IPv4_IPv6
Guía 20 - Transición IPv4_IPv6
Guía 21 - Gestión de Incidentes

Fuente: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

4.4. RESOLUCIÓN N° 001519 DE 24 DE AGOSTO DE 2020

“Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos”.

ARTÍCULO 1. Objeto. La presente resolución tiene por objeto expedir los lineamientos que deben atender los sujetos obligados para cumplir con la publicación y divulgación de la información señalada en la Ley 1712 del 2014, estableciendo los criterios para la estandarización de contenidos e información, accesibilidad web, seguridad digital, datos abiertos y formulario electrónico para Peticiones, Quejas, Reclamos, Sugerencias y

Denuncias (PQRSD).

Directrices de accesibilidad web - Anexo 1 Resolución 1519
Estándares de publicación y divulgación información - Anexo 2 Resolución 1519
Condiciones mínimas técnicas y de seguridad digital - Anexo 3 Resolución 1519
Requisitos mínimos de datos abiertos - Anexo 4 Resolución 1519

FUENTE:
https://gobiernodigital.mintic.gov.co/692/articles-178657_resolucion_1519_2020.pdf

4.5. RESOLUCIÓN 40199 DE 28 DE JUN 2021

Por la cual se adoptan los lineamientos del modelo de gobierno de tecnologías de la información y del modelo de gobierno de datos del sector minero energético.

ARTÍCULO 1o. OBJETO. Adoptar los lineamientos del modelo de Gobierno de tecnologías de la información y del modelo de Gobierno de datos del sector minero-energético, entendidos como dominios (componentes) de la arquitectura empresarial sectorial, mediante los cuales se brindan directrices para la implementación de esquemas de gobernabilidad de tecnologías de información y de datos y se adoptan las políticas que permitan alinear los procesos y planes de las instituciones con los del sector.

Esto, con el fin de gestionar el uso de los datos, toma de decisiones, divulgación de información, operaciones sectoriales, sistemas de información y articulación con las diferentes estrategias, basados en información, analítica de datos y servicios tecnológicos, cumpliendo con todos los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, en adelante “MinTIC”, y los que se expidan por las autoridades nacionales.

Fuente:
https://www.minenergia.gov.co/documents/10180//23517//48979-RESOLUCI%C3%93N+40199+DEL+28-6-2021.pdf

4.6. REGLAMENTO TÉCNICO DE INSTALACIONES ELÉCTRICAS - RETIE

En cumplimiento del artículo 2° de la Constitución Nacional, les corresponde a las autoridades de la República proteger a todas las personas residentes en Colombia en su vida, honra y bienes. En tal sentido el Ministerio de Minas y Energía como máxima autoridad en materia energética, adopta los reglamentos técnicos orientados a garantizar la protección de la vida de las personas contra los riesgos que puedan provenir de los bienes y servicios relacionados con el sector a su cargo.

El objeto fundamental de este reglamento es establecer las medidas tendientes a garantizar

la seguridad de las personas, de la vida tanto animal como vegetal y la preservación del medio ambiente; previniendo, minimizando o eliminando los riesgos de origen eléctrico. Sin perjuicio del cumplimiento de las reglamentaciones civiles, mecánicas y fabricación de equipos

Los objetivos de un sistema de puesta a tierra (SPT) son: La seguridad de las personas, la protección de las instalaciones y la compatibilidad electromagnética.

Las funciones de un sistema de puesta a tierra son:

a. Garantizar condiciones de seguridad a los seres vivos.
b. Permitir a los equipos de protección despejar rápidamente las fallas.
c. Servir de referencia común al sistema eléctrico.
d. Conducir y disipar con suficiente capacidad las corrientes de falla, electrostática y de rayo.
e. Transmitir señales de RF en onda media y larga.
f. Realizar una conexión de baja resistencia con la tierra y con puntos de referencia de los equipos.

Fuente: https://www.minenergia.gov.co/retie

4.7. ESTANDAR ANSI / TIA-942

El estándar de infraestructura de telecomunicaciones ANSI / TIA-942 adoptado a nivel mundial para centros de datos, especifica los requisitos mínimos para centros de datos y cubre toda la infraestructura física, incluida, entre otras:

La ubicación del sitio
Arquitectura
Electricidad
Mecánica
Seguridad contra incendios
Telecomunicaciones
Seguridad y otros requerimientos.

Fuente:
https://tiaonline.org/products-and-services/tia942certification/ansi-tia-942-standard/

4.8. NORMA TECNICA COLOMBIANA NTC 2885 de 2009

Dentro de la Norma Técnica Colombiana NTC 2885 numeral 5.2, los incendios se clasifican en:

- Clase A, son incendios de materiales combustibles comunes, como la madera, tela,

papel, caucho y muchos plásticos.
- Clase B, son incendios de líquidos inflamables, líquidos combustibles, grasas de petróleo, alquitrán, aceites, pinturas a base de aceite, disolventes, lacas, alcoholes y gases inflamables.
- Clase C, son incendios que involucran equipos eléctricos energizados.
- Clase D, son incendios de metales combustibles como el magnesio, titanio, circonio, sodio, litio y potasio.
- Clase K, son incendios de electrodomésticos que involucran combustibles para cocinar (aceites y grasas vegetales o animales).

Todo mantenimiento y recarga al sistema contra incendio debe tener un registro visible de etiqueta o rotulo sujeta en forma segura que indique el mes y año en que se hizo el mantenimiento, el nombre de la persona que realizo el trabajo, y el nombre de la agencia. (NTC 2885). Los mantenimientos especializados deben ser realizados cada seis meses y cada año se debe realizar una inspección completa al sistema, que incluye aceptación y pruebas de:

- Revisión de los componentes mecánicos
- Pruebas a la red de tuberías
- Revisión de los componentes eléctricos
- Unidad de control
- Cableados
- Circuitos auxiliares
- Pruebas preliminares al sistema
- Pruebas al sistema operacional
- Notificación a la oficina receptora de alarmas y a todo el personal involucrado que la prueba ha sido completada.

Los sistemas fijos están cubiertos por las siguientes normas:

NFPA 11, Standard for Low-, Medium-, and High Expansion Foam;
NFPA 12, Standard on Carbon Dioxide Extinguishing Systems;
NFPA 12 A, Standard on Halon 130 Fire Extinguishing Systems,
NFPA 13, Standard for the Installation of Sprinkler Systems;
NFPA 14, Standard for the Installation of Stand pipe and Hose Systems;
NFPA 15, Standard for Water Spray Fixed Systems for Fire Protection;
NFPA 16, Standard for the Installation of Foam-Water Sprinkler and Foam-Water Spray Systems;
NFPA 17, Standard for Dry Chemical Extinguishing Systems;
NFPA 17A, Standard for Wet Chemical Extinguishing Systems;
NFPA 96, Standard for Ventilation Control and Fire Protection of Commercial Cooking Operations;
NFPA 750, Standard on Water Mist Fire Protection Systems;
NFPA 2001, Standard on Clean Agent Fire Extinguishing Systems.

5. ANALISIS DE LA INFORMACIÓN

Con el objeto de realizar la auditoría interna a los procesos de las tecnologías de la información y comunicaciones – TIC IPSE 2021, se recopilaron varias fuentes de información:

5.1. Fuente de Análisis SECOP 2017-2021 mayo.

Con referencia al SECOP como fuente primaria de registro de contratos, realice la descarga de todos los registros de contratos del IPSE desde 2017 a 2021 mayo, con un total de 548 registros (Contratos).

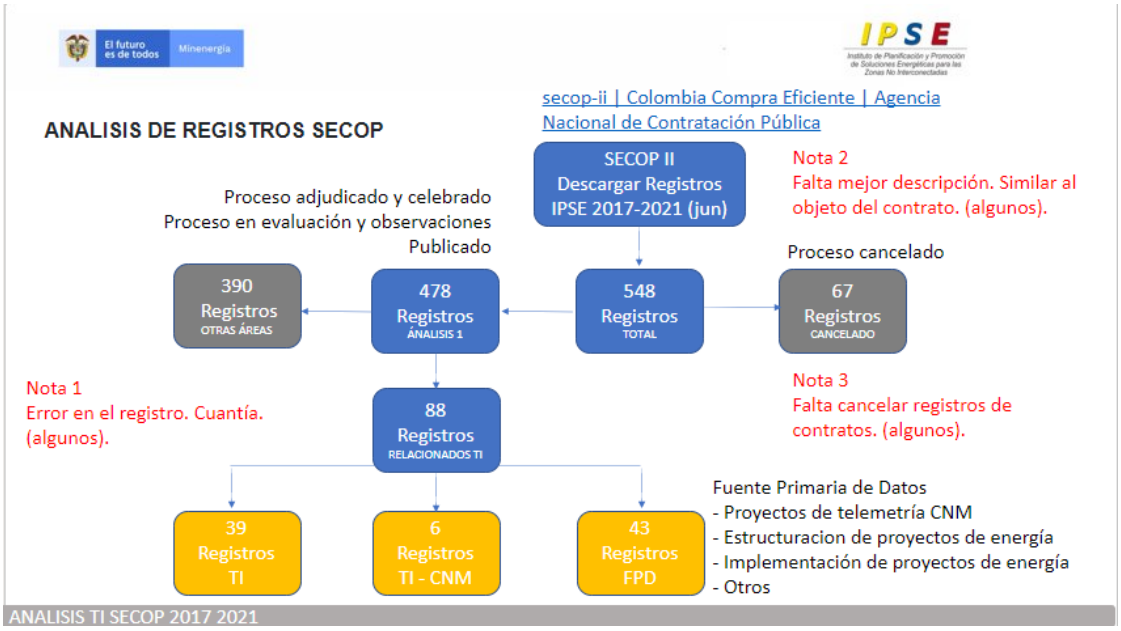


Figura. Registros de contratos IPSE 2017-2021may. Fuente SECOP.

Luego de revisión, se identifican 45 registros de contratos de TI IPSE otros 43 que no son directamente contratos de TI, pero si generar información primaria de bases de datos en Zonas No Interconectadas que debe ser integrada a los sistemas de información del IPSE, y se construye la herramienta “Matriz de Análisis SECOP v1.xlsx”

Por tanto, esta base de datos de información son fuente de interés para el análisis de planeación, inversiones y funcionamiento de las Tecnologías de la Información y Comunicaciones del IPSE.

5.2. Fuente de Contexto TI Sectorial

Análisis del documento de RESOLUCIÓN 40199 DE 28 DE JUN 2021, por la cual se adoptan los lineamientos del modelo de gobierno de tecnologías de la información y del modelo de gobierno de datos del sector minero energético.

...Articulo 1. Objeto: *Adoptar los lineamientos del modelo de gobierno de tecnologías de la información y del modelo de gobierno de datos del sector minero energético, entendidos como dominios (componentes) de arquitectura empresarial sectorial, mediante los cuales se brinda directrices para la implementación de esquemas de gobernabilidad de tecnologías de la información y de datos y se adoptan las políticas que permitan alinear los procesos, planes de las instituciones con los del sector.*

Esto, con el fin de gestionar el uso de los datos de toma de decisiones, divulgación de la información, operaciones sectoriales, sistemas de información y articulación con las diferentes estrategias, basados en información, analítica de datos y servicios tecnológicos, cumpliendo con todos los lineamientos de Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia en adelante "MinTIC", y los que se expidan por las autoridades nacionales...

Fuente*:* Resolución 40199 de 28 de jun 2021

5.3. Fuente de información PETIC IPSE

El Plan Estratégico de las Tecnologías de la Información y Comunicaciones es el artefacto que se utiliza para expresar la Estrategia de TI.

Incluye una visión, unos principios, unos indicadores, un mapa de ruta, un plan de comunicación y una descripción de todos los demás aspectos (financieros, operativos, de manejo de riesgos, etc.) necesarios para la puesta en marcha y gestión del plan estratégico.

Con referencia al objeto de la auditoria de realizo el análisis del documento PLAN ESTRATEGICO DE TECNOLOGIA PETI IPSE 2020 – 2023. Proceso: Gestión TICS 2021

PETI IPSE 2018

PETI IPSE Actual 2020-2023

Fuente: Plan Estratégico de Tecnologías de la Información y las Comunicaciones – IPSE

5.4. Fuente de información Proceso de gestión TIC

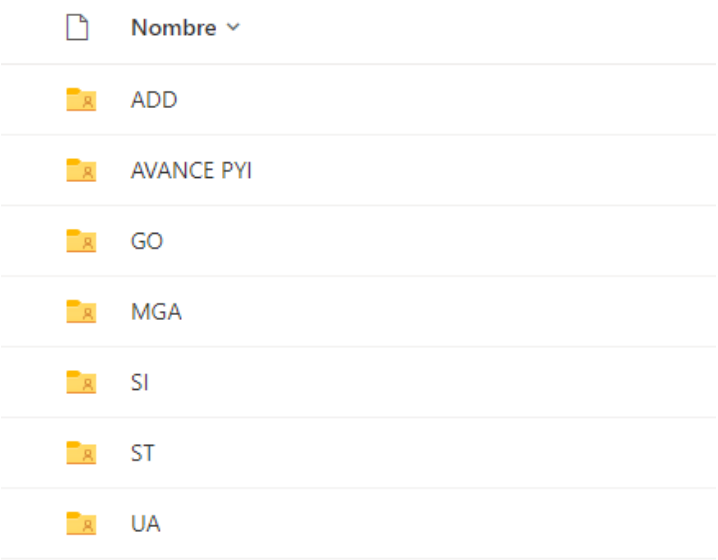
Análisis de los documentos del proceso y procedimientos de Gestión de TIC, descargados del Sistema de gestión Integral del IPSE:

IPSE-TIC-C01 Caracterización del proceso de Gestión de TICs Objetivo: Gestionar estratégicamente las necesidades de innovación en tecnología, seguridad y operatividad que requieran las partes interesadas, con el fin de apoyar el cumplimiento de los objetivos institucionales en el marco de la estrategia de Gobierno Digital.
IPSE-TIC-P02 Procedimiento seguridad y privacidad de la información. Objetivo: Proteger los activos de información del IPSE soportados por los servicios de TI, enfocándose en la confidencialidad, integridad y la continuidad de los mismos. Administración, identidad y cuentas de usuario. Backup's de información y transferencia. Protección software y hardware.
IPSE-TIC-P03 Procedimiento de innovación tecnológica.

Objetivo: Gestionar en el IPSE con eficiencia (gestión de los recursos) y eficacia (consecución de los objetivos) las capacidades tecnológicas de una manera continua, permitiendo al Proceso de Gestión de TIC innovar y mejorar las diferentes estrategias para atender los requerimientos de las partes interesadas tomando como referencia el mercado.
IPSE-TIC-P03 Procedimiento de soporte y mantenimiento hardware y software. Objetivo: Soportar y mantener el hardware y software del IPSE

5.5. Fuente de información Respuesta 1 – PETIC

Mediante radicado IPSE-20211340021263 el grupo de TICS IPSE realizo la primera entrega de información relacionada con el PETI 2020-2023:



Pantalla de las carpetas con información PETI entregadas mmediante radicado IPSE-20211340021263

5.6. Fuente de información Respuesta 2 – AE ERP

Mediante radicado IPSE-20211330028773 el grupo de TICS IPSE realizo la segunda entrega de información relacionada con preguntas relacionadas con Arquitectura Empresarial, el sistema de información ORFEO y el software de gestión empresarial ERP SICOF.

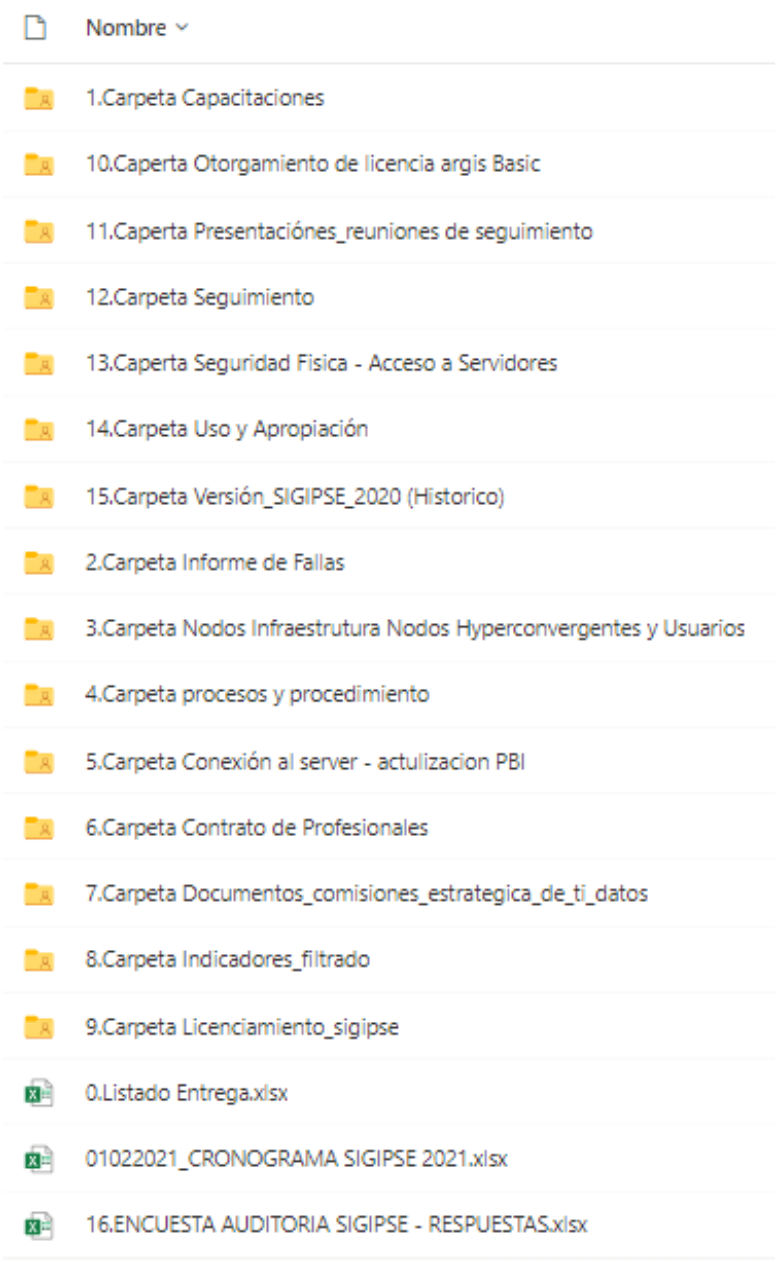
5.7. Fuente de información Respuesta 3 – CNM

Mediante correo electrónico del Centro Nacional de Monitoreo del IPSE se recopilo información técnica de los sistemas de telemetría CNM:

Pantalla de archivos con información CNM.

5.8. Fuente de información Respuesta 4 –SIGIPSE

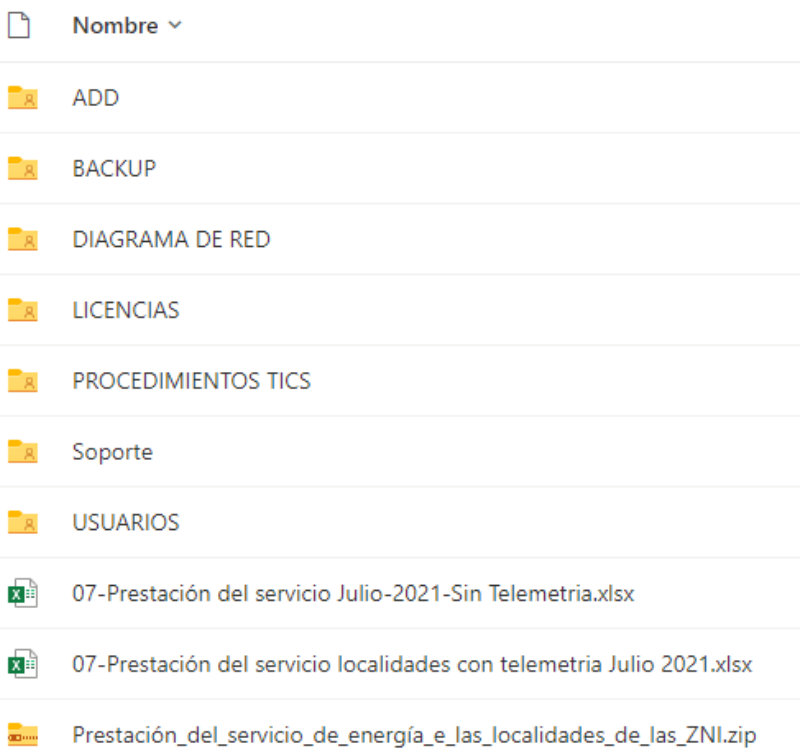
Mediante correo electrónico del grupo de Gestión TICS se recopilo información técnica del sistema de información geográfica SIGIPSE:



Pantalla de carpetas con información SIGIPSE.

5.9. Fuente de información Respuesta 5 – TIC

Mediante correo electrónico del grupo de Gestión TICS se recopilo información técnica del sistema de información geográfica SIGIPSE y TELEMETRIA:



Pantalla de carpetas con información SIGIPSE y TELEMETRIA.

6. OBSERVACIONES Y RECOMENDACIONES DE AUDITORIA

La auditoría fue realizada por el equipo multidisciplinario de la Oficina de Control Interno que cumplen con los requisitos y competencias como auditores de, garantizando su objetividad, imparcialidad e independencia, concebida para agregar valor y mejorar las operaciones de la entidad, esperando contribuir a cumplimiento de los objetivos institucionales, aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos, de la gestión del riesgo y de los controles.

Como resultado de la auditoria a tecnologías de la información y comunicaciones del IPSE con base en el análisis de la información descrita en el ítem 5 y las visitas técnicas a los centros de datos del IPSE, se formulan las siguientes observaciones que se señalan a continuación:

6.1. CENTRO DE DATOS IPSE CALLE 100 – INFRAESTRUCTURA TECNOLÓGICA

- **DESCRIPCIÓN DE LA VISITA**

Visita técnica realizada el 16 de septiembre 2021 al centro de datos IPSE CALLE 100, para el análisis de la infraestructura tecnológica, identificando los riesgos con su evidencia fotográfica y descripción de la observación:

Personal entrevistado:

- Ingeniera Paola Montenegro
- Ingeniero Miller Rodríguez - Líder de Proceso (Virtualmente).

- **OBSERVACIONES AL CENTRO DE DATOS IPSE CALLE 100**

Riesgo de falla de continuidad de negocio por fallas en centro de datos CALLE 100.

En la visita técnica al centro de datos CALLE 100, se observaron riesgos tecnológicos que impactan la continuidad del negocio de la entidad. Como referencia técnica y normativa para el análisis, tenemos la Guía No 10 del Modelo de Seguridad y Privacidad de la Información - MSPI para la continuidad del Negocio, y el estándar ANSI / TIA-942 para centro de datos.

Para el caso del centro de datos CALLE 100 de la Entidad, el impacto negativo de una interrupción del servicio se clasifica en Nivel A y es de operación critica para el negocio. Por tanto, al tener una falla en el centro de datos, la función del negocio no puede realizarse, materializándose el riesgo de falla continuidad del servicio.

El Centro de datos CALLE 100, es la plataforma tecnológica que contiene los servidores, equipos de comunicaciones y equipos de seguridad firewall para la operación de los

sistemas de información:

Sistema	Descripción
ORFEO	Sistema de gestión documental.
ERP SICOF	Sistema de planificación de recursos. Nomina, Inventario, Recursos humamos, etc.
SIGIPSE	Sistema de Información Geográfica del IPSE
GLPI	Mesa de ayuda. Soporte técnico TI del IPSE.
SGI	Sistema de Gestión Integral.
Maquina Virtuales	Escritorios virtuales para todos los funcionarios y contratistas de la entidad.
FORTINET	Sistema de seguridad Firewall.
Internet	Servicio de internet.
Intranet	Servicio de intranet
Publico	Carpetas compartidas para almacenamiento y compartir documentos de la entidad.

Consecuentemente el riesgo de materialización de una falla de la plataforma tecnológica en el centro de datos, impacta directamente la continuidad del negocio del IPSE.

Para el desarrollo del análisis técnico de la auditoria de TI del centro de datos CALLE 100, se identificaron amenazas de seguridad interna, y externa, ambiente físico, protección de activos de información, protección de la información y protección de recursos humanos, identificando las siguientes observaciones:

6.1.1. Falla de seguridad de control de acceso al centro de datos.

Se observa que la puerta de acceso al centro de datos permanece abierta, debido a que el biométrico no está funcionando en la actualidad, razón por la cual se desactivo el actuador magnético para que la puerta permanezca abierta, lo cual no cumple con el estándar de seguridad de la Norma ANSI / TIA 942 para centros de datos.

En consecuencia, se evidencia el riesgo de seguridad de control de acceso físico al centro de datos que contienen los equipos de comunicaciones, seguridad y servidores de los sistemas de información: ORFEO, máquinas de escritorios virtuales, ERP, Sistema de Información geográfica IPSE, Sistemas de Gestión Integral y Mesa de Ayuda GLPI.

Recomendación.
Se recomienda aplicar el procedimiento IPSE-TIC-04 “Soporte y mantenimiento hardware y software” del sistema de gestión integral SGI del IPSE, que inicia con la actividad “*Planear mantenimiento para la vigencia*”, y seguir los lineamientos de la norma ANSI / TIA 942 para centros de datos. Que incluya la revisión y puesta en servicio del sistema de control de acceso del centro de datos.

6.1.2. Falta de mantenimiento de las UPS's del centro de datos.

En la visita de inspección técnica realizada, se observa que las UPS's del centro de datos, presentan alarma de ***"Batería descargada",*** evidenciando la falta de seguimiento al mantenimiento de las mismas, con un riesgo de colapso total del centro de datos por falla de suministro eléctrico, en consecuencia se presenta una alta probabilidad de materializarse el riesgo de pérdida de información de los sistemas: ORFEO, máquinas de escritorios virtuales, ERP, Sistema de Información geográfica IPSE, Sistemas de Gestión Integral y Mesa de Ayuda GLPI, al incumplir el estándar de requerimientos eléctricos de UPS de la Norma ANSI / TIA 942 para centros de datos.

Recomendación. Se recomienda aplicar el procedimiento IPSE-TIC-04 "Soporte y mantenimiento hardware y software" del sistema de gestión integral SGI del IPSE, que inicia con la actividad "*Planear mantenimiento para la vigencia*", y seguir los lineamientos de la norma ANSI / TIA 942 para centros de datos. Que incluya la revisión, reemplazo de baterías y puesta en servicio de las UPS's del centro de cómputo.

6.1.3. Sistema contra incendios sin registro de mantenimiento ni recarga en el centro de datos.

En el recorrido de inspección técnica al centro de datos, se evidencia que el sistema contra incendio ECARO-25 no tiene registro de mantenimiento ni de recarga, el cual es de obligatorio cumplimiento de acuerdo la Norma Técnica Colombiana NTC 2885. De igual manera se incumple el estándar ANSI / TIA 942 en seguridad contra incendios.

Adicionalmente, se observó en el centro de datos almacenamiento de cajas de cartón y cables que son precursores de incendio Clase A (Incendios de materiales combustibles comunes, como la madera, tela, papel, caucho y muchos plásticos).

En consecuencia, se identifica un riesgo para la vida, activos y continuidad del negocio en el centro de datos, debido a la falta de mantenimiento del sistema contra incendios.

Recomendación. Se recomienda aplicar el procedimiento IPSE-TIC-04 "Soporte y mantenimiento hardware y software" del sistema de gestión integral SGI del IPSE, que inicia con la actividad "*Planear mantenimiento para la vigencia*", y seguir los lineamientos de la norma ANSI / TIA 942 para centros de datos. Que incluya la revisión, recarga y puesta en servicio del sistema contraincendios del centro de datos.

6.1.4. Riesgo de desconexión eléctrica y corto circuito en el centro de datos.

En visita técnica al centro de datos, se observa que los cableados eléctricos en los racks (gabinetes de equipos) presentan riesgos eléctricos, debido a cableado eléctrico desorganizado, tomas eléctricas sobrecargadas, multitomas no reguladas para centros de datos, adaptadores de alimentación de equipos colgados del cable mismo y cables eléctricos que pasan entre racks sin protecciones, evidenciando riesgo de desconexión eléctrica y corto circuito, incumpliendo: el Reglamento Técnico de Instalaciones Eléctricas - RETIE, estándar ANSI / TIA 942 en electricidad el centro de datos y NTC 2885 riesgo de incendio Clase C (incendios que involucran equipos eléctricos energizados).

El riesgo eléctrico tiene como consecuencia la desconexión forzada de los equipos de comunicaciones, seguridad y servidores del centro de datos, con riesgo indisponibilidad y perdida de información de los sistemas ORFEO, máquinas de escritorios virtuales, ERP, Sistema de Información geográfica IPSE, Sistemas de Gestión Integral y Mesa de Ayuda GLPI.

El riesgo de corto circuito por sobrecarga de multitomas eléctricas, cableados inadecuados y multitomas genéricas tiene como consecuencia la probabilidad de incendio por corto circuito. Riesgo de incendio Clase C.

Recomendación. Se recomienda aplicar el procedimiento IPSE-TIC-04 “Soporte y mantenimiento hardware y software” del sistema de gestión integral SGI del IPSE, que inicia con la actividad “*Planear mantenimiento para la vigencia*”, y seguir los lineamientos de la norma ANSI / TIA 942 para centros de datos. Que incluya la adecuación y revisión de cableado eléctrico del centro de datos ajustado al reglamento técnico de instalaciones eléctricas RETIE.

6.1.5. Riesgo de desconexión de red de datos de los equipos en el centro de datos.

En visita técnica al centro de datos, se observa que los cableados de red de datos en los racks (gabinetes de equipos) presentan riesgos desconexión, debido a cableados de datos desorganizados, con cables UTP y de fibra óptica enredados entre ellos y con los cables de energía, cables irregularmente atravesados por encima de los racks y por el piso, que no cumple con estándar ANSI / TIA 942 en telecomunicaciones.

El riesgo de desconexión de red de datos de los equipos de comunicaciones, seguridad y servidores, tiene consecuencia sobre la continuidad del negocio del IPSE debido al riesgo de la no disponibilidad de los sistemas: ORFEO, máquinas de escritorios virtuales, ERP, Sistema de Información geográfica IPSE, Sistema de Gestión Integral y Mesa de Ayuda GLPI.

Recomendación.

Se recomienda aplicar el procedimiento IPSE-TIC-04 “Soporte y mantenimiento hardware y software” del sistema de gestión integral SGI del IPSE, que inicia con la actividad “*Planear mantenimiento para la vigencia*”, y seguir los lineamientos de la norma ANSI / TIA 942 para centros de datos. Que incluya la adecuación y revisión de cableado de red de datos y organización de equipos y racks del centro de datos.

6.1.6. Riesgo de desconexión de red del equipo FortiAnalizer del sistema de seguridad Firewall del centro de datos.

Se evidencia riesgo de desconexión e indisponibilidad de la red de seguridad Firewall del centro de datos, debido a la tensión sobre el cable de red y conector al equipo de seguridad FortiNET FortiAnalizer, porque se amarro un cable al extremo del conector del equipo. Incumpliendo la norma ANSI / TIA-942 en telecomunicaciones y seguridad para centros de datos.

Recomendación. Se recomienda aplicar el procedimiento IPSE-TIC-04 “Soporte y mantenimiento hardware y software” del sistema de gestión integral SGI del IPSE, que inicia con la actividad “*Planear mantenimiento para la vigencia*”, y seguir los lineamientos de la norma ANSI / TIA 942 para centros de datos. Que incluya la adecuación y revisión de cableado de red de datos y organización de equipos y racks del centro de datos.

6.1.7. No se evidencio el diagrama de arquitectura de red de la infraestructura tecnológica del centro de datos.

Dentro de la información solicitada por esta auditoria al grupo de TI, no se evidencia el diagrama de arquitectura de red donde se identifiquen los equipos de red, servidores y sus conexiones: Router de internet, el firewall Fortinet, switch Aruba HP, Juniper SRX300, Juniper SRX100, switch red LAN, servidores y terminales de datos CALLE 100.

El diagrama entregado por el grupo de TIC como respuesta a la solicitud, no es un diagrama de arquitectura de red, este es un diagrama de racks y no corresponde a la arquitectura de red.

Al no tener un diagrama de arquitectura de red actualizado se tiene el riesgo de no poder identificar como se relacionan los equipos para realizar análisis y seguimiento al funcionamiento de la red.

Recomendación. Se recomienda aplicar el procedimiento IPSE-TIC-04 “Soporte y mantenimiento hardware

y software" del sistema de gestión integral SGI del IPSE, que inicia con la actividad "*Planear mantenimiento para la vigencia*", y seguir los lineamientos de la norma ANSI / TIA 942 para centros de datos.

Que incluya la revisión, organización y levantamiento de información de toda la infraestructura lógica y física del centro de datos con los diagramas técnicos de arquitectura de red y diagramas de ubicación en los racks.

6.2. CENTRO DE DATOS CNM – INFRAESTRUCTURA TECNOLÓGICA

- **DESCRIPCIÓN DE LA VISITA**

Visita técnica realizada el 16 de septiembre 2021 al centro de datos IPSE CNM, para el análisis de la infraestructura tecnológica, identificando los riesgos con su evidencia fotográfica y descripción de la observación:

Personal entrevistado:

- Ingeniera Paola Montenegro
- Ingeniero Miller Rodríguez - Líder de Proceso (Virtualmente).
- Ingeniero Álvaro Alexander Mossos - CNM

- **OBSERVACIONES AL CENTRO DE DATOS IPSE CNM.**

Riesgo de falla de continuidad de negocio por fallas en centro de datos CNM.

En la visita técnica al centro de datos CNM, se observaron riesgos tecnológicos que impactan la continuidad del negocio de la entidad. Como referencia técnica y normativa para el análisis, tenemos la Guía No 10 del Modelo de Seguridad y Privacidad de la Información - MSPI para la continuidad del Negocio, y el estándar ANSI / TIA-942 para centro de datos.

Para el caso del centro de datos CNM de la Entidad, el impacto negativo de una interrupción del servicio se clasifica en Nivel A y es de operación critica para el negocio. Por tanto, al tener una falla en el centro de datos, la función del negocio no puede realizarse, materializándose el riesgo de falla continuidad del servicio.

El Centro de datos CNM, es la plataforma tecnológica que contiene los servidores, equipos de comunicaciones y equipos de seguridad firewall para la operación de los sistemas de información:

Sistema	Descripción
PRIME READ	Sistema de información misional para la gestión de telemetría de medida de energía en centrales de generación en ZNI. Dato certificado código de medida.
ION ENTERPRISE	Sistema de información misional para la gestión de telemetría

	en tiempo real de medida de energía en centrales de generación en ZNI.
GESTEL	Sistema de información misional para integrar los datos de medida de energía en centrales de generación y potenciales energéticos en ZNI. Sistema generador de reportes de telemetría del Centro Nacional de Monitoreo.
SIIETE	Sistema de información asociada a la generación de energía de las ZNI.
FORTINET	Sistema de seguridad Firewall.
Internet	Servicio de internet.
Ultima milla	Servicio de comunicación de los sistemas de telemetría Prime Read e ION Enterprise con el telepuerto satelital para comunicación con las estaciones de monitoreo en ZNI.

Consecuentemente el riesgo de materialización de una falla de la plataforma tecnológica en el centro de datos, impacta directamente la continuidad del negocio del IPSE.

Para el desarrollo del análisis técnico de la auditoria de TI del centro de datos CNM, se identificaron amenazas de seguridad interna, y externa, ambiente físico, protección de activos de información, protección de la información y protección de recursos humanos, identificando las siguientes observaciones:

6.2.1. Falla de seguridad de control de acceso al centro de datos.

Se observa que la puerta de acceso al centro de datos permanece abierta, debido a que el aire acondicionado no funciona y se percibe alta temperatura ambiental, entonces como medida de recirculación de aire se mantiene la puerta abierta (Se observa el letrero "*Favor no cerrar esta puerta*"), lo cual no cumple con el estándar de seguridad de la Norma ANSI / TIA 942 para centros de datos.

En consecuencia, se evidencia el riesgo de seguridad de control de acceso físico al centro de datos CNM y los racks que contienen equipos de comunicaciones, seguridad y servidores de los sistemas de información de telemetría: Prime Read, ION Enterprise, GESTEL y SIIETE.

Recomendación.
Se recomienda aplicar el procedimiento IPSE-TIC-04 "Soporte y mantenimiento hardware y software" del sistema de gestión integral SGI del IPSE, que inicia con la actividad "*Planear mantenimiento para la vigencia*", y seguir los lineamientos de la norma ANSI / TIA 942 para centros de datos. Que incluya la revisión y puesta en servicio del sistema de control de acceso del centro de datos.

6.2.2. Falta de mantenimiento de la UPS del centro de datos.

En la visita de inspección técnica realizada al centro de datos del CNM, se evidencia la falta de seguimiento al mantenimiento del sistema UPS, con un riesgo de colapso total del centro de datos por falla de suministro eléctrico, en consecuencia, se presenta una alta probabilidad de materializarse el riesgo de pérdida de información de los sistemas: Prime Read, ION Enterprise, GESTEL y SIIETE, al incumplir el estándar de requerimientos eléctricos de UPS de la Norma ANSI / TIA 942 para centros de datos.

Un mantenimiento del UPS se trata de un diagnóstico y análisis del estado actual de la UPS, e incluye la revisión de parámetros del equipo, limpieza, revisión de baterías y pruebas técnicas de funcionamiento. Dando mayor vida útil a la UPS, seguridad de que la infraestructura de misión crítica siempre sea operativa y ahorro de costos por pedidas de productividad. El no realizar el mantenimiento preventivo de la UPS genera riegos de falla se servicio de energía al centro de datos CNM

Recomendación. Se recomienda aplicar el procedimiento IPSE-TIC-04 “Soporte y mantenimiento hardware y software” del sistema de gestión integral SGI del IPSE, que inicia con la actividad “*Planear mantenimiento para la vigencia*”, y seguir los lineamientos de la norma ANSI / TIA 942 para centros de datos. Que incluya la revisión, reemplazo de baterías y puesta en servicio de las UPS’s del centro de cómputo.

6.2.3. Se observa que el centro de datos no tiene un sistema contra incendios tipo fijo, de operación automática, propio de un centro de datos.

En el recorrido de inspección técnica, se observa que dentro del centro de datos solo se tiene un extintor portátil tipo HFCF y un sensor de humo de la alarma del edificio Torre Av 82, que no cumple con el estándar ANSI / TIA 942 para el sistema de protección contra incendios para centros de datos.

Con el sistema actual de extintor portátil, en el caso de iniciarse un incendio en el centro de datos, no va a ser posible que una persona entre a tratar de apagar el fuego porque el extintor está ubicado dentro del centro de datos, o porque el personal de la oficina no esté en jornada laboral.

Adicionalmente, se observó en el centro de datos almacenamiento de cajas de cartón y cables que son precursores de incendio Clase A (Incendios de materiales combustibles comunes, como la madera, tela, papel, caucho y muchos plásticos).

En consecuencia, se identifica un riesgo para la vida, activos y continuidad del negocio en el centro de datos CNM, debido a la falta de un sistema contra incendios tipo fijo de operación automática, especializado para centros de datos.

Recomendación.

Se recomienda aplicar el procedimiento IPSE-TIC-04 “Soporte y mantenimiento hardware y software” del sistema de gestión integral SGI del IPSE, que inicia con la actividad “*Planear mantenimiento para la vigencia*”, y seguir los lineamientos de la norma ANSI / TIA 942 para centros de datos.

El CNM no tiene un sistema contra incendios tipo fijo y de operación automática necesario para un centro de datos.

6.2.4. Falla del aire acondicionado del centro de datos.

En la visita técnica realizada al centro de datos CNM, se observa que el aire acondicionado instalado de marca LG LT-C302FLEO de 30.000 Btu no está en funcionamiento, este aire fue instalado en 2006 y actualmente es obsoleto sin posibilidad de mantenimiento.

Al no tener en funcionamiento un sistema de aire acondicionado, no se puede mantener la temperatura adecuada de forma estable y controlada que es fundamental para el funcionamiento de equipos y que contribuya a tener un centro de datos robusto, confiable y durable, incumpliendo estándar ANSI / TIA 942 para el control de temperatura en el centro de datos.

Debido a no tener aire acondicionado en el centro de datos CNM, se tomaron tres medidas irregulares:

(1) Instalaron un extractor de aire caliente, con una manguera extractora pegada a la ventana con cinta.
(2) Dejaron la ventana permanente abierta, con entrada de polvo y humedad externa.
(3) Dejaron la puerta de acceso permanentemente abierta, sin control de acceso.

En consecuencia, se evidencia el riesgo de falla y daño en los servidores con posible pérdida de información de los sistemas del CNM, por exposición a temperaturas no controladas, polvo y humedad.

Recomendación.

Se recomienda aplicar el procedimiento IPSE-TIC-04 “Soporte y mantenimiento hardware y software” del sistema de gestión integral SGI del IPSE, que inicia con la actividad “*Planear mantenimiento para la vigencia*”, y seguir los lineamientos de la norma ANSI / TIA 942 para centros de datos.

El sistema de aire acondicionado debe ser reemplazado, debido a que el sistema actual no funciona y no tiene posibilidad de mantenimiento.

6.2.5. Alto nivel de contaminación por polvo en los servidores, equipos de comunicación y equipos de seguridad del centro de datos.

En la visita técnica al centro de datos CNM, se evidencia una alta contaminación por polvo en los servidores, equipos de comunicaciones, puertos de comunicación y demás componentes electrónicos, incumpliendo estándar ANSI / TIA 942.

La contaminación es debido a que la ventana del centro de datos está permanentemente abierta, porque el aire acondicionado no funciona y el extractor de aire caliente que está pegado con cinta, y no deja cerrar la ventana, ocasionando una entrada continua de polvo y humedad del exterior.

El alto nivel de polvo, causa riesgo de inestabilidad en el centro de datos; por cortos eléctricos por polvo, deterioro de la vida útil de los equipos por falla en ventiladores internos, falla en lectores ópticos, falla por aislamiento de los puertos de comunicación y riesgo de pérdida de datos en los servidores del centro de datos CNM.

Adicionalmente, se observó que en la vigencia 2021 se instaló un equipo de almacenamiento SAN en el centro de datos CNM, adquirido mediante el contrato 120-2020 lote 1 operación 41428183, sin tener en cuenta las fallas de aire acondicionado, alto nivel de contaminación por polvo y riesgo eléctrico del sitio.

.

Recomendación.
Se recomienda aplicar el procedimiento IPSE-TIC-04 “Soporte y mantenimiento hardware y software” del sistema de gestión integral SGI del IPSE, que inicia con la actividad de planear mantenimiento para la vigencia, y seguir los lineamientos de la norma ANSI / TIA 942 para centros de datos. Que incluya la revisión y limpieza especializada de todos los equipos afectados por polvo, así como la corrección de todas las fallas que causaron la alta contaminación por polvo en el centro de datos.

6.2.6. Riesgo de desconexión eléctrica y corto circuito en el centro de datos.

En visita técnica al centro de datos, se observa que los cableados eléctricos en los racks (gabinetes de equipos) presentan riesgos eléctricos, debido a cableado eléctrico desorganizado, tomas eléctricas sobrecargadas, multitomas no reguladas para centros de datos, cables eléctricos que llegan a los racks pegados con cinta transparente al piso y cables eléctricos que pasan entre racks sin protecciones, evidenciando riesgo de desconexión eléctrica y corto circuito, incumpliendo: el Reglamento Técnico de Instalaciones Eléctricas - RETIE, estándar ANSI / TIA 942 en electricidad el centro de datos y NTC 2885 riesgo de incendio Clase C (incendios que involucran equipos eléctricos energizados).

El riesgo eléctrico tiene como consecuencia la desconexión forzada de los equipos de comunicaciones, seguridad y servidores del centro de datos, con riesgo indisponibilidad y perdida de información de los sistemas de telemetría del CNM: PrimeREAD, ION Enterprise, GESTEL y SIIETE.

El riesgo de corto circuito por sobrecarga de multitomas eléctricas, cableados inadecuados y multitomas genéricas tiene como consecuencia la probabilidad de incendio por corto circuito. Riesgo de incendio Clase C.

Recomendación.

Se recomienda aplicar el procedimiento IPSE-TIC-04 “Soporte y mantenimiento hardware y software” del sistema de gestión integral SGI del IPSE, que inicia con la actividad “*Planear mantenimiento para la vigencia*”, y seguir los lineamientos de la norma ANSI / TIA 942 para centros de datos. Que incluya la adecuación y revisión de cableado eléctrico del centro de datos ajustado al reglamento técnico de instalaciones eléctricas RETIE.

6.2.7. Riesgo de desconexión de red de datos de los equipos en el centro de datos.

En visita técnica al centro de datos, se observa que los cableados de red de datos en los racks (gabinetes de equipos) presentan riesgos desconexión, debido a cableados de datos desorganizados, con cables UTP y de fibra óptica enredados entre ellos y con los cables de energía, cables irregularmente atravesados por encima de los racks y por el piso, que no cumple con estándar ANSI / TIA 942 en telecomunicaciones.

El riesgo de desconexión de red de datos de los equipos de comunicaciones, seguridad y servidores, tiene consecuencia sobre la continuidad del negocio del IPSE debido al riesgo de la no disponibilidad de los sistemas de telemetría: PrimeREAD, ION Enterprise, GESTEL y SIIETE.

Recomendación. Se recomienda aplicar el procedimiento IPSE-TIC-04 “Soporte y mantenimiento hardware y software” del sistema de gestión integral SGI del IPSE, que inicia con la actividad “*Planear mantenimiento para la vigencia*”, y seguir los lineamientos de la norma ANSI / TIA 942 para centros de datos. Que incluya la adecuación y revisión de cableado de red de datos y organización de equipos y racks del centro de datos.

6.3. CENTRO DE DATOS SOACHA – INFRAESTRUCTURA TECNOLÓGICA

- **DESCRIPCIÓN DE LA VISITA**

Visita técnica realizada el 21 de septiembre 2021 al centro de datos IPSE SOACHA, para el análisis de la infraestructura tecnológica, identificando los riesgos con su evidencia fotográfica y descripción de la observación:

Personal entrevistado:

- Ingeniera Paola Montenegro
- Ingeniero Miller Rodríguez - Líder de Proceso (Virtualmente).

- **OBSERVACIONES AL CENTRO DE DATOS IPSE SOACHA.**

Riesgo de falla de continuidad de negocio por fallas en centro de datos de SOACHA.

En la visita técnica al centro de datos SOACHA, se observaron riesgos tecnológicos que impactan la continuidad del negocio de la entidad. Como referencia técnica y normativa para el análisis, tenemos la Guía No 10 del Modelo de Seguridad y Privacidad de la Información - MSPI para la continuidad del Negocio, y el estándar ANSI / TIA-942 para centro de datos.

Para el caso del Centro de datos de SOACHA, el impacto negativo de una interrupción del servicio se clasifica en Nivel A y es de operación critica para el negocio. Por tanto, al tener una falla en el centro de datos, la función del negocio no puede realizarse, materializándose el riesgo de falla continuidad del servicio.

El Centro de datos de SOACHA, es la plataforma tecnológica que contiene los servidores, equipos de comunicaciones y equipos de seguridad firewall para la operación **DRP Plan de Recuperación de Desastres** de los sistemas de información:

Sistema DRP	Descripción
ORFEO	Sistema de gestión documental.
ERP SICOF	Sistema de planificación de recursos. Nomina, Inventario, Recursos humamos, etc.
SIGIPSE	Sistema de Información Geográfica del IPSE
GLPI	Mesa de ayuda. Soporte técnico TI del IPSE.
SGI	Sistema de Gestión Integral.
Maquina Virtuales	Escritorios virtuales para todos los funcionarios y contratistas de la entidad.
FORTINET	Sistema de seguridad Firewall.
Internet	Servicio de internet.
Intranet	Servicio de intranet
Publico	Carpetas compartidas para almacenamiento y compartir documentos de la entidad.

Consecuentemente el riesgo de materialización de una falla de la plataforma tecnológica en el centro de datos, impacta directamente la continuidad del negocio del IPSE.

Para el desarrollo del análisis técnico de la auditoria de TI del centro de datos de SOACHA, se identificaron amenazas de seguridad interna, y externa, ambiente físico, protección de activos de información, protección de la información y protección de recursos humanos, identificando las siguientes observaciones:

6.3.1. Falla en la acometida eléctrica de red normal al centro de datos.

En la visita técnica, se realizó el recorrido de inspección de la acometida eléctrica, evidenciando una falla en el ducto EMT que protege cable de acometida eléctrica. Se observa que el ducto esta desprendido de los puntos de fijación y sostiene su peso sobre el cable eléctrico, esta carga del ducto con sus bordes metálicos sobre el cable es irregular,

generando un riesgo eléctrico, al no cumplir RETIE - Reglamento Técnico de Instalaciones Eléctricas.

Recomendación. Se recomienda aplicar el procedimiento IPSE-TIC-04 “Soporte y mantenimiento hardware y software” del sistema de gestión integral SGI del IPSE, que inicia con la actividad “*Planear mantenimiento para la vigencia*”, y seguir los lineamientos de la norma ANSI / TIA 942 para centros de datos. Que incluya la adecuación y revisión de cableado eléctrico, puesta a tierra y sistema pararrayos del centro de datos ajustado al reglamento técnico de instalaciones eléctricas RETIE.

6.3.2. Falla en el sistema de puesta a tierra que ingresa al tablero eléctrico del centro de datos.

En la visita de inspección técnica, se observa que el Sistema de Puesta a Tierra - STP que ingresa al tablero del centro de datos presenta evidencia de falla por sobrecalentamiento, sulfatación del cable de cobre y en el patio no existen cajas de inspección de varillas de malla a tierra, incumpliendo Reglamento Técnico de Instalaciones Eléctricas - RETIE y el estándar ANSI / TIA 942.

Teniendo como referencia que el centro de datos de SOACHA fue construido en el año 2018, es obligatorio que la instalación eléctrica cumpla con certificación RETIE, y al no cumplirlo se evidencia un alto riesgo eléctrico para las personas, instalaciones, infraestructura tecnológica, incompatibilidad electromagnética y sistemas de información, con riesgo de pérdida de la información y nos exponemos a la pérdida de garantía de los equipos.

Recomendación. Se recomienda aplicar el procedimiento IPSE-TIC-04 “Soporte y mantenimiento hardware y software” del sistema de gestión integral SGI del IPSE, que inicia con la actividad “*Planear mantenimiento para la vigencia*”, y seguir los lineamientos de la norma ANSI / TIA 942 para centros de datos. Que incluya la adecuación y revisión de cableado eléctrico, puesta a tierra y sistema pararrayos del centro de datos ajustado al reglamento técnico de instalaciones eléctricas RETIE.

6.3.3. No existe sistema de pararrayos en el edificio del centro de datos.

En la visita de inspección técnica al centro de datos de SOACHA una vez realizado el recorrido por el predio, se observa que no existe sistema de protección de pararrayos en la edificación, incumpliendo Reglamento Técnico de Instalaciones Eléctricas - RETIE y el estándar ANSI / TIA 942.

La infraestructura y unión de las tierras físicas de telecomunicaciones, en conjunto con los sistemas de tierra física eléctrica y de los pararrayos, forman un sistema completo del edificio, el cual ayuda a proteger a equipos y personal de voltajes peligrosos. Un mal sistema tierra física para los cuartos de telecomunicaciones puede producir voltajes inducidos que afectan los sistemas de telecomunicaciones, ocasionando fallas y caídas en los equipos, hasta llegar incluso a la pérdida total de ellos o de la información que contienen.

Al no cumplir con el estándar de infraestructura de telecomunicaciones para centros de datos TIA/EIA-942, se tiene el riesgo de pérdida de la información de nuestro centro de datos y nos exponemos a la pérdida de garantía de los equipos.

Recomendación. Se recomienda aplicar el procedimiento IPSE-TIC-04 “Soporte y mantenimiento hardware y software” del sistema de gestión integral SGI del IPSE, que inicia con la actividad “*Planear mantenimiento para la vigencia*”, y seguir los lineamientos de la norma ANSI / TIA 942 para centros de datos. Que incluya la adecuación y revisión de cableado eléctrico, puesta a tierra y sistema pararrayos del centro de datos ajustado al reglamento técnico de instalaciones eléctricas RETIE.

6.3.4. La infraestructura de red eléctrica del centro de datos presenta riesgo de corto circuito e incendio.

En la revisión de infraestructura eléctrica del centro de datos SOACHA, se evidencia que en el tablero de energía se tienen varias protecciones eléctricas breaker fijadas con cinta de enmascarar en la posición de OFF, lo que no permite pasarlos a la posición activa de ON, esta situación irregular es debido a que debajo del piso falso hay un amarre de cables eléctricos con las puntas de cobre expuestas con riesgo de corto circuito e incendio, incumpliendo Reglamento Técnico de Instalaciones Eléctricas - RETIE.

Recomendación. Se recomienda aplicar el procedimiento IPSE-TIC-04 “Soporte y mantenimiento hardware y software” del sistema de gestión integral SGI del IPSE, que inicia con la actividad “*Planear mantenimiento para la vigencia*”, y seguir los lineamientos de la norma ANSI / TIA 942 para centros de datos. Que incluya la adecuación y revisión de cableado eléctrico, puesta a tierra y sistema pararrayos del centro de datos ajustado al reglamento técnico de instalaciones eléctricas RETIE.

6.3.5. Almacenamiento irregular de combustible en el centro de datos, incumpliendo la norma NTC 2885 de 2009.

En la visita de inspección técnica realizada, se observa almacenamiento irregular de

combustible en dos tanques plásticos, no certificados para este fin, sin marcación y con riesgo de inflamabilidad a lado de la puerta de centro de datos, con riesgo de incendio Clase B (Incendios de líquidos inflamables, líquidos combustibles, grasas de petróleo, alquitrán, aceites, pinturas a base de aceite, disolventes, lacas, alcoholes y gases inflamables), incumpliendo norma NTC 2885 de 2009.

Recomendación. Se recomienda aplicar el procedimiento IPSE-TIC-04 “Soporte y mantenimiento hardware y software” del sistema de gestión integral SGI del IPSE, que inicia con la actividad “*Planear mantenimiento para la vigencia*”, y seguir los lineamientos de la norma ANSI / TIA 942 para centros de datos. Que incluya adecuación de almacenamiento de combustible y mantenimiento de la planta de generación de energía de respaldo del centro de datos.

6.3.6. Falla en el sistema de trasferencia automática de energía del centro de datos.

En la visita de inspección técnica realizada, se observa que la unidad de control “ComAp InteLite AMF 20” de la planta de generación de energía de respaldo del centro de datos, tiene desconectadas las señales de los sensores de voltaje, por tanto, en caso de falla del servicio energía, la planta alterna de energía no se activara automáticamente, incumpliendo a guía de instalación y operación del fabricante ComAp.

Al no funcionar la planta de respaldo ante una falla de suministro eléctrico, los servidores y demás equipos del centro de datos van presentar un apagado forzado, perdida de información y discontinuidad del servicio del centro de datos.

Recomendación. Se recomienda aplicar el procedimiento IPSE-TIC-04 “Soporte y mantenimiento hardware y software” del sistema de gestión integral SGI del IPSE, que inicia con la actividad “*Planear mantenimiento para la vigencia*”, y seguir los lineamientos de la norma ANSI / TIA 942 para centros de datos. Que incluya adecuación de almacenamiento de combustible y mantenimiento de la planta de generación de energía de respaldo del centro de datos.

6.3.7. Falla de seguridad de control de acceso al centro de datos.

Se observa que la puerta de acceso al centro de datos permanece abierta, debido a que el sistema de control de acceso está inhabilitado, con el actuador magnético desmontado, porque no se tiene configurado las huellas en el biométrico y no se tiene información de la llave de la chapa de la puerta lo cual no cumple con el estándar de seguridad de la Norma ANSI / TIA 942 para centros de datos.

En consecuencia, se evidencia el riesgo de seguridad de control de acceso físico al centro

de datos que contienen equipos de comunicaciones, seguridad y servidores de respaldo DRP (Plan de Recuperación de Desastres) de los sistemas de información del dentro de datos IPSE CALLE 100.

Recomendación. Se recomienda aplicar el procedimiento IPSE-TIC-04 “Soporte y mantenimiento hardware y software” del sistema de gestión integral SGI del IPSE, que inicia con la actividad “*Planear mantenimiento para la vigencia*”, y seguir los lineamientos de la norma ANSI / TIA 942 para centros de datos. Que incluya la revisión y puesta en servicio del sistema de control de acceso del centro de datos.

6.3.8. No se evidencia que el sistema de video seguridad este en funcionamiento en el centro de datos.

Se observa que el equipo de grabación DVR del sistema de video seguridad del centro de datos está dentro del gabinete de comunicaciones puesto en el piso y no se evidencia que el sistema esté en funcionamiento, con el riesgo de no tener registro de ingreso o de actividades realizadas dentro del centro de cómputo, mediante el sistema video seguridad.

Recomendación. Se recomienda aplicar el procedimiento IPSE-TIC-04 “Soporte y mantenimiento hardware y software” del sistema de gestión integral SGI del IPSE, que inicia con la actividad “*Planear mantenimiento para la vigencia*”, y seguir los lineamientos de la norma ANSI / TIA 942 para centros de datos. Que incluya la revisión y puesta en servicio del sistema de video seguridad del centro de datos.

6.3.9. El rack de comunicaciones del centro de datos no tiene una organización técnica de cableados de energía y comunicaciones.

En la visita técnica al centro de datos, se observa que el cableado de energía, datos y fibra óptica están desorganizados, hay cables eléctricos con bolsas plásticas amarradas y se tiene equipos puestos en el piso, incumpliendo con estándar ANSI / TIA 942 en telecomunicaciones.

Como consecuencia de no tener una organización técnica de cableados y ubicación de equipos, se tiene el riesgo de desconexión de equipos de comunicación, servidores y sistemas de información.

Recomendación. Se recomienda aplicar el procedimiento IPSE-TIC-04 “Soporte y mantenimiento hardware

y software" del sistema de gestión integral SGI del IPSE, que inicia con la actividad "*Planear mantenimiento para la vigencia*", y seguir los lineamientos de la norma ANSI / TIA 942 para centros de datos.

Que incluya la adecuación y revisión de los cableados de red de datos y de energía del centro de datos.

6.3.10. Alto nivel de contaminación por polvo en los servidores, equipos de comunicación y equipos de seguridad del centro de datos.

En la visita técnica al centro de datos de SOACHA, se evidencia una alta contaminación por polvo en los servidores, equipos de comunicaciones, puertos de comunicación y demás componentes electrónicos, incumpliendo estándar ANSI / TIA 942 en las actividades de planificación de mantenimientos a la infraestructura del centro de datos.

La contaminación por polvo en el centro de datos es debido a la falla del filtro de aire del sistema de aire acondicionado, por falta de mantenimiento.

El alto nivel de polvo, causa riesgo de inestabilidad en el centro de datos; por cortos eléctricos por polvo, deterioro de la vida útil de los equipos por falla en ventiladores internos, falla en lectores ópticos, falla por aislamiento de los puertos de comunicación y riesgo de pérdida de datos en los servidores del centro de datos de SOACHA.

Recomendación.

Se recomienda aplicar el procedimiento IPSE-TIC-04 "Soporte y mantenimiento hardware y software" del sistema de gestión integral SGI del IPSE, que inicia con la actividad de planear mantenimiento para la vigencia, y seguir los lineamientos de la norma ANSI / TIA 942 para centros de datos.

Que incluya la revisión y limpieza especializada de todos los equipos afectados por polvo, así como la corrección de todas las fallas que causaron la alta contaminación por polvo en el centro de datos.

6.3.11. El centro de datos del CNM no está integrado al centro de datos alterno de SOACHA.

En desarrollo de esta auditoría, se evidencia que el centro de datos del CNM no está integrado al centro de datos de SOACHA.

El centro de datos de SOACHA se implementó mediante contrato IPSE 124-2017, como el modelo de centro de datos alterno, de funcionamiento proactivo para casos de incidencia mayor, para respaldo de la infraestructura tecnológica de los centros de datos del IPSE, sirviendo como contingencia y sitio alterno de respaldo de información; sin embargo, se observa que actualmente solo se tiene integrado el centro de datos del IPSE CALLE 100.

Consecuentemente, no se tiene respaldo en en centro de datos de SOACHA de la

infraestructura e información del centro de datos del CNM, que es la plataforma tecnológica que contiene los sistemas de información misional de telemetría de medición de energía en las Zonas No Interconectadas.

Recomendación. Teniendo en cuenta las fallas críticas del centro de datos del CNM descritas en el numeral 6.2 de este informe, se recomienda realizar el respaldo del funcionamiento de los sistemas de información de telemetría del CNM IPSE, analizado las tres opciones posibles: Respaldo en el centro de datos de SOACHA, respaldo en la nube o respaldo en otro centro de datos en modo de colocación.

6.4. PLAN ESTRATÉGICO DE TECNOLÓGICAS DE LA INFORMACIÓN - PETI

- **DESCRIPCIÓN DEL CONTEXTO PETI IPSE**

El Plan Estratégico de las Tecnologías de la Información y Comunicaciones es el artefacto que se utiliza para expresar la **Estrategia de TI**.

En el Manual de Gobierno Digital, en la etapa de IMPLEMENTAR, se cita[1]:

"...***Una vez la entidad cuente con el PETI y el plan de seguridad y privacidad de la información,*** *en donde se definieron los proyectos y se establecieron las actividades, responsables, tiempos de ejecución y recursos para la ejecución de la política, ésta debe desarrollar dichas iniciativas o proyectos..."*

En el documento *"G.ES.06 Guía para la construcción del PETI"* se presenta la metodología que **las entidades deben seguir** para diseñar e implementar un Plan Estratégico de las Tecnologías de Información PETI. El objetivo de esta guía es orientar a la Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, durante la elaboración de su Plan Estratégico de Tecnologías de la Información.

La evolución del Plan Estratégico de las Tecnologías de la Información y Comunicaciones del IPSE, se ha desarrollado en dos fases:

Fase 1 PETI 2018	La primera versión del PETI 2018 se desarrolló dentro del alcance del contrato IPSE 062-2017.
Fase 2 PETI 2020-2023	La segunda versión del PETI 2020-2023 del 13-10-2020, la desarrollo "Equipo de TICS" basada en: - La plantilla *de* MinTIC *"TDxT-Plantilla_PETI_PLUS.docx". Fuente:* https://mintic.gov.co/arquitecturati/630/w3-article-15031.html

[1] Fuente: https://gobiernodigital.mintic.gov.co/portal/Politica-de-Gobierno-Digital/Manual-de-Gobierno-Digital/

	- PETI IPSE 2018.

Y con vigencia 2021, el IPSE tiene dos contratos relacionados con la actualización de PETI:

Contrato IPSE 008-2021	*"Obligación especifica 2: Apoyar, en la actualización de su Plan Estratégico de Tecnologías de la Información 2020-2023 – PETIC 2020-2023"*
Contrato IPSE 057-2021	*"Obligación especifica 2: Brindar apoyo en la gestión administrativa derivada de la actualización Plan Estratégico de Tecnologías de la Información PETIC 2020-2023".*

En desarrollo de la auditoria, el grupo de TICS IPSE realizo entrega de información relacionada con el PETI 2020-2023 mediante radicado ORFEO No 20211340021263, la cual es el objeto de análisis.

- **OBSERVACIONES AL PLAN ESTRATÉGICO DE TECNOLÓGICAS DE LA INFORMACIÓN - PETI**

El documento "PLAN ESTRATEGICO DE TECNOLOGIA - PETI 2020-2023" esta desactualizado e incompleto, no cumple con la guía *"G.ES.06 Guía para la construcción del PETI"*: no releja la situación actual (AS-IS), no contiene la situación objetivo (TO-BE), y en el capítulo "*Portafolio de iniciativas, proyectos y mapa de ruta"*, indica cinco (5) proyectos que no coinciden con el proyecto de inversión de TIC IPSE *"Fortalecimiento de las Tecnologías de la Información y las Comunicaciones TIC de IPSE como referente de información para ZNI – Código BPIN 2019011000150*".

Res

Fuente: ORFEO No 20211340021263

PETI IPSE Actual 2020-2023	

Documentos de análisis

Para el desarrollo del análisis del documento “PLAN ESTRATEGICO DE TECNOLOGIA - PETI 2020-2023”, se tienen en cuenta los anexos relacionados en la respuesta del grupo de TI IPSE ORFEO No 20211340021263 y los lineamientos de MinTIC. Identificando las siguientes observaciones específicas:

6.4.1. El IPSE no tiene en funcionamiento una herramienta software de Arquitectura Empresarial AE.

El IPSE adquirió desde el año 2018 mediante contrato 062-2017 la herramienta de software MEGA OPEX, la cual es fundamental para el manejo y administración de la información de Arquitectura Empresarial y el PETI.

Esta auditoria pudo evidenciar que en el IPSE no se administra, actualiza y/o usa la herramienta software MEGA OPEX, de acuerdo a la respuesta data por del grupo de TI IPSE con Rad. 20211330028773.

“*El software de Arquitectura Empresarial MEGA HOPEX en estos momentos no se administra, actualiza y/o usa dicha herramienta…”*

De otra parte, tampoco se usó la herramienta software de Arquitectura Empresarial enviada por MME al IPSE dentro del marco del programa de fortalecimiento institucional del Sector Minero Energético Colombiano - Proyecto BID 3594 OC/CO, la cual rechazo el IPSE con evidencia en el Rad. 20181340010291.

CARLOS ANDRÉS CANTE PUENTES
Viceministro de minas
Ministério de Minas y Energía
Calle 43 N° 57 – 31 CAN Bogotá.
Bogotá D.C., Colombina

ASUNTO: Respuesta comunicación Herramienta Arquitectura Empresarial Rad: 2018036325.

Según comunicación recibida, nos fue informado: "En el marco del programa fortalecimiento Institucional del Sector Minero Energético colombiano – (BID 3594 OC/CO)" se definió trabajar sobre una plataforma llamada Visual Paradigm para centralizar el repositorio de arquitectura empresarial, adicionalmente que hay una licencia disponible para uso y operación de IPSE."

Agradecemos su oferta; queremos informar que el IPSE ya cuenta con una herramienta software como repositorio para Arquitectura Empresarial "MEGA HOPEX", previamente adquirida bajo el CONTRATO 062 – 2017 firmado el 12 DE OCTUBRE DE 2017, que tiene como objeto "Definición, diseño e implementación de la Arquitectura Empresarial para el IPSE", por ello el IPSE no requiere utilizar el licenciamiento de Visual Paradigm.

Atentamente,

NEILA LUZ BALETA MIZAR
Directora General (E)

Proyectó: Deyber Erickson Rodríguez Alvarez – Contratista Grupo tecnología y Sistemas de Información IPSE
Reviso: Angelina Toloza Pabón – Coordinadora Grupo tecnología y Sistemas de Información IPSE

En consecuencia, al no tener en uso una herramienta especializada en Arquitectura Empresarial, se evidencia que el IPSE maneja el modelo de Arquitectura Empresarial y el Plan Estratégico de Tecnologías de la Información - PETI en carpetas de documentos Word y Excel, con riesgo de duplicidad de documentos, inconsistencias, reprocesos, contradicciones y confusiones, en el manejo y administración de la información de Arquitectura Empresarial y el PETI.

Recomendación.
Se recomienda usar una herramienta de software para el manejo y administración de la información de Arquitectura Empresarial y el Plan Estratégico de Tecnologías de la Información PETI del IPSE, y cargar todos los artefactos que se definen en la situación actual, situación objetivo, brechas y mapa de ruta de la entidad en tecnologías de la información.

6.4.2. Los documentos técnicos del capítulo "SITUACION ACTUAL" del PETI IPSE 2020-2023, están desactualizados y no reflejan la situación actual AS-IS del IPSE.

Mediante radicado IPSE-20211340021263 el grupo de TICS IPSE realizo la entrega de documentos relacionados en el PETI IPSE 2020-2023, los cuales una vez analizados en

esta auditoria se evidencia:

- Los documentos del capítulo "*SITUACION ACTUAL*" del numeral 4.1.3 "*Servicios de TI*" relacionados del PETI IPSE 2020-2023 están desactualizados y no reflejan la situación actual AS-IS del IPSE, no incluye la infraestructura tecnología actualizada del CNM, ni el centro de datos de SOACHA.

- El documento "*Cadena_Valor_TI_LI.GO.04_V1.0."* del capítulo "SITUACION ACTUAL" del numeral 4.2.1 "Cadena de Valor de TI" del PETI IPSE 2020-2023, describe un listado de proyectos por 24.471.803.000 de pesos, los cuales son diferentes a los proyectos indicados en el *"Portafolio de iniciativas, proyectos y mapa de ruta"* por 4.650.000.000 de pesos del mismo PETI 2020-2023.

- El documento "*Tablero_Indicadores_LI.GO.11_V1.0.xlsx*." del capítulo "SITUACION ACTUAL" del numeral 4.2.2 "Indicadores y Riesgos" del PETI IPSE 2020-2023, describe los formatos de indicadores de estrategia, gobierno, información y servicios tecnológicos, pero no se observa el diligenciamiento de los formatos de indicadores ni la descripción de los riesgos.

- El documento *"Directorio_Sistemas_Informacion_LI.SIS.02_V1.0"* del capítulo "SITUACION ACTUAL" del numeral 4.3.1 "Herramientas de Análisis" del PETI IPSE 2020-2023, esta desactualizado. El directorio no incluye el actual sistema de información SIG IPSE, ni el ERP SICOF, ni el modelo DRP de los sistemas de información del centro de datos de SOACHA.

- El documento *"Mapa de Ruta Ipse v7.0-2"* del capítulo "*SITUACION ACTUAL*" del numeral 4.3.1 "*Herramientas de Análisis*" del PETI IPSE 2020-2023, es el documento de la versión PETI 2018 con 36 proyectos por $30.750.000.000 de pesos que no se ejecutó y luego fue reemplazado en la versión PETI 2020-2023, pero sin actualizar el documento "*Mapa de Ruta IPSE*".

- El documento "*Definición_Arquitectura_SIS-INFV1.0"* del capítulo "SITUACION ACTUAL" del numeral 4.3.1 "Herramientas de Análisis" del PETI IPSE 2020-2023, esta desactualizado. El directorio no incluye el actual sistema de información SIG IPSE, ni el ERP SICOF, ni el modelo DRP de los sistemas de información del centro de datos de SOACHA.

- El documento "*AsIs_SIS_Artef_V0.7"* del capítulo "*SITUACION ACTUAL*" del numeral 4.4 *"Sistema de Información*" del PETI IPSE 2020-2023, esta desactualizado. El documento no incluye el actual sistema de información SIG IPSE, ni el ERP SICOF, ni el modelo DRP de los sistemas de información del centro de datos de SOACHA.

Se evidencia que se usaron los anexos técnicos de "*Situación Actual AS-IS*" del PETI 2018 para construir el PETI 2020-2023, sin realizar la actualización correspondiente, en consecuencia, el documento PETI 2020-2023 que establece la estrategia de TI

(Tecnologías de la Información), no refleja la "*Situación Actual AS-IS*" del IPSE y no cumple con los lineamientos del Manual de Gobierno Digital.

Por tanto, tener un documento PETI desactualizado y/o incompleto es un riesgo para la toma de decisiones de planeación, análisis y seguimiento en el área de Tecnologías de la Información y Comunicaciones del IPSE.

Recomendación. Se recomienda realizar la actualización del PETI IPSE y sus componentes de documentos técnicos Artefactos del PETI, ajustados a los lineamientos de MinTIC según la G.ES.06 Guía para la Construcción del PETI– Planeación de la Tecnología para la Transformación Digital julio de 2019. Donde debe contener la **situación actual AS-IS**, la situación objetivo TO-BE, las brechas y el mapa de ruta de la entidad en Tecnologías de la Información y sus documentos técnicos actualizados.

6.4.3. En el documento PETI IPSE 2020-2023 no está el capítulo de SITUACIÓN OBJETIVO TO-BE, el cual hace parte fundamental de la estructura de un Plan Estratégico de Tecnologías de la Información de una entidad.

Al comparar la forma y contenido del documento PETI 2020-2023, se observa que se tuvo como referencia el documento "*TDxT-Plantilla_PETI_PLUS*" que contiene el Capitulo 5 **Situación Objetivo TO-BE**, de la guía "*G.ES.06 Guía para la construcción del PETI de MinTIC, sin embargo,* este capitulo no fue desarrollado en el documento PETI 2020-2023.

Se evidencia que el documento PETI 2020-2023 que establece la estrategia de TI (Tecnologías de la Información), no contiene la "*Situación Objetivo TO-BE*" del IPSE y no se cumple con el desarrollo de la guía "*G.ES.06 Guía para la construcción del PETI de MinTIC".*

Por tanto, tener un documento PETI incompleto es un riesgo para la toma de decisiones de planeación, análisis y seguimiento en el área de Tecnologías de la Información y Comunicaciones del IPSE.

Recomendación. Se recomienda realizar la actualización del PETI IPSE y sus componentes de documentos técnicos Artefactos del PETI, ajustados a los lineamientos de MinTIC según la G.ES.06 Guía para la Construcción del PETI– Planeación de la Tecnología para la Transformación Digital julio de 2019. Donde debe contener la situación actual AS-IS, **la situación objetivo TO-BE**, las brechas y el mapa de ruta de la entidad en Tecnologías de la Información y sus documentos técnicos actualizados.

6.4.4. En el capítulo de "*Identificación de Hallazgos y Brechas"*, del documento PETI IPSE 2020-2023, no se tiene un identificador ID por cada brecha, por tanto, no es posible identificar en el portafolio de proyectos, que brechas se cierran con cada proyecto del mapa de ruta.

Al revisar el documento PETI 2020-2023, se observa que el capítulo de "*Identificación de Hallazgos y Brechas" página 42,* se tienen descritas las brechas de negocio, brechas de sistemas de información, brechas de información y brechas de servicios tecnológicos, sin identificación de un ID por cada brecha.

Entonces, debido a que en el modelo del PETI IPSE 2020-2023 no se tiene un identificador ID por cada brecha, no es posible asociar a cada proyecto del mapa de ruta que brecha soluciona y no se cumple con el desarrollo de la guía "*G.ES.06 Guía para la construcción del PETI de MinTIC".*

Recomendación. Se recomienda realizar la actualización del PETI IPSE y sus componentes de documentos técnicos Artefactos del PETI, ajustados a los lineamientos de MinTIC según la G.ES.06 Guía para la Construcción del PETI– Planeación de la Tecnología para la Transformación Digital julio de 2019. Donde debe contener la situación actual AS-IS, la situación objetivo TO-BE, **las brechas** y el mapa de ruta de la entidad en Tecnologías de la Información y sus documentos técnicos actualizados.

6.4.5. El documento PETI 2020-2023 indica cuatro listados de proyectos TI, que no están alineados entre ellos.

En el capítulo "*Portafolio de iniciativas y mapa de ruta"* del documento PETI IPSE 2020-2023, se observa que proyectos indicados en la ***"****Matriz de relación programas, portafolio proyectos" no coinciden a los indicados en la "Hoja de Ruta",* ni en los documentos anexos: *"Cadena_Valor_TI_LI.GO.04_V1.0*." y "*Mapa de Ruta Ipse v7.0-2*"; evidenciando que los documentos que presentan los proyectos de TI no están alineados, causando confusión en el documento que define la estrategia de TI de la entidad.

Los documentos de análisis para planificar, evaluar y realizar seguimiento a los proyectos relacionados en el PETI IPSE 2020- 2023 son:

- Matriz de relación de programas, portafolio proyectos. Pagina 49.
- Hola de Ruta. Pagina 52.
- Documento "*Cadena_Valor_TI_LI.GO.04_V1.0"*. Anexo al PETI 2020-2023 y coincide con el Plan de Inversión TI IPSE ORFEO No 20211340021263.
- *Documento "Mapa de Ruta Ipse v7.0-2".* Anexo al PETI 2020-2023.

Estos cuatro documentos que presentan los proyectos de TI del PETI 2020-2023, deben estar alineados entre ellos y con el Plan de Inversión de TI de la Entidad, pero se observan que todos son diferentes, en proyectos y en valores.

Al realizar el análisis de estos documentos, se observa que ni la relación de proyectos ni los valores asociados, están alineados en los cuatro apartes del mismo documento PETI IPSE 2020-2023, evidenciado, que en este documento PETI no está ajustado a los lineamientos de MinTIC. Por tanto, el documento PETI 2020-2023 de la estrategia de tecnologías de la información de IPSE no refleja la planeación de las iniciativas, proyectos y mapa de ruta de la entidad.

Recomendación.

Se recomienda realizar la actualización del PETI IPSE y sus componentes de documentos técnicos Artefactos del PETI, ajustados a los lineamientos de MinTIC según la G.ES.06 Guía para la Construcción del PETI– Planeación de la Tecnología para la Transformación Digital julio de 2019. Donde debe contener la situación actual AS-IS, la situación objetivo TO-BE, las brechas y el **mapa de ruta** de la entidad en Tecnologías de la Información y sus documentos técnicos actualizados.

6.5. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

6.5.1. El documento publicado en el SGI de *"Políticas de Seguridad y Privacidad de la Información del IPSE*" esta desactualizado.

El documento de *"Políticas de Seguridad y Privacidad de la Información del IPSE*" con resolución 20171300002585 del 13 de septiembre 2017, publicado en el Sistema de Gestión Integral y aprobado por la alta dirección, esta desactualizado y no refleja la situación actual de los servicios de tecnologías de la información del IPSE, no contiene las políticas de seguridad y privacidad de la información de los sistemas de información: ERP SICOF, SIG IPSE, Sistemas misionales de telemetría del CNM, ni los sistemas de información instalados en el centro de datos de SOACHA del Plan de Recuperación de Desastres DRP.

Adicionalmente, se observa en el informe 3 de supervision del contrato IPSE 050-2018 con Rad. 20191340064143 página 15, que el IPSE recibió el documento entregable "*Política de seguridad y privacidad de la información - Manual de políticas específicas, CORREGIDO. (Se dejo el del IPSE como base y se complementó con el manual de políticas específicas que, propuesto el Contratista, y se unifico en este documento)"*, sin embargo, en desarrollo de esta auditoria se evidencio que está actualización no fue publicado al Sistema de Gestión Integral SGI con la correspondiente aprobación por la alta dirección del IPSE.

Por tanto, tener un documento desactualizado "*Políticas de Seguridad y Privacidad de la Información del IPSE*" es un riesgo para la toma de decisiones de planeación, análisis y seguimiento en el área de Tecnologías de la Información y Comunicaciones de la entidad.

Recomendación.

Se recomienda seguir los lineamientos del Manual de Gobierno Digital[2], que el módulo de implementar indica "***Una vez la entidad cuente con el PETI y el plan de seguridad y privacidad de la información**, en donde se definieron los proyectos y se establecieron las actividades, responsables, tiempos de ejecución y recursos para la ejecución de la política, ésta debe desarrollar dichas iniciativas o proyectos, aplicando lineamientos que*

[2] Manual de Gobierno Digital. El Manual de Gobierno Digital es el documento que establece los lineamientos y estándares de los componentes de la política (TIC para el Estado y TIC para la Sociedad) y de los habilitadores transversales (arquitectura, seguridad y privacidad de la información y servicios ciudadanos digitales).

corresponden a los componentes ***TIC para el Estado y TIC para la Sociedad***".

Se recomienda seguir los lineamientos de MinTIC del Modelo de Seguridad y Privacidad de la Información - MSPI, que imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital. Y se desarrolla mediante el Documento Maestro del Modelo de Seguridad y Privacidad de la Información y sus guías de orientación. Lo debe desarrollar el líder o encargado de Seguridad de la Información con el apoyo de toda la estructura organizacional.

6.6. PROCEDIMIENTO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - BACKUPS DE INFORMACION Y TRANSFERENCIA

6.6.1 El procedimiento de backups registrado en el Sistema de Gestión Integral -SGI código IPSE-TIC-P02 esta desactualizado.

El procedimiento de Procedimiento de Privacidad y Seguridad de la Información, para Backups de información y transferencia, registrado en el Sistema de Gestión Integral SGI del IPSE con código IPSE-TIC-P02 esta desactualizado y no refleja en modelo actual de procedimiento de Backups realizado por el grupo de tecnologías de la información del IPSE.

Por tanto, se evidencia que la actual política de Backups del IPSE no coincide con el procedimiento IPSE-TIC-P02, "Procedimiento de Privacidad y Seguridad de la Información - Backup's de información y transferencia", en consecuencia, el procedimiento IPSE-TIC-P02 esta desactualizado y debe ser actualizado al modelo actual

Recomendación.

Se recomienda realizar la revisión del proceso IPSE-TIC-C01 de Gestión de TICS y sus procedimientos para actualización a la situación actual de IPSE:

- IPSE-TIC-P02 Procedimiento seguridad y privacidad de la información.
- IPSE-TIC-P03 Procedimiento de innovación tecnológica.
- IPSE-TIC-P03 Procedimiento de soporte y mantenimiento hardware y software.

Y realizar el cambio de procedimiento IPSE-TIC-P02 "Procedimiento de Privacidad y Seguridad de la Información - Backup's de información y transferencia", en el módulo de Backus de información.

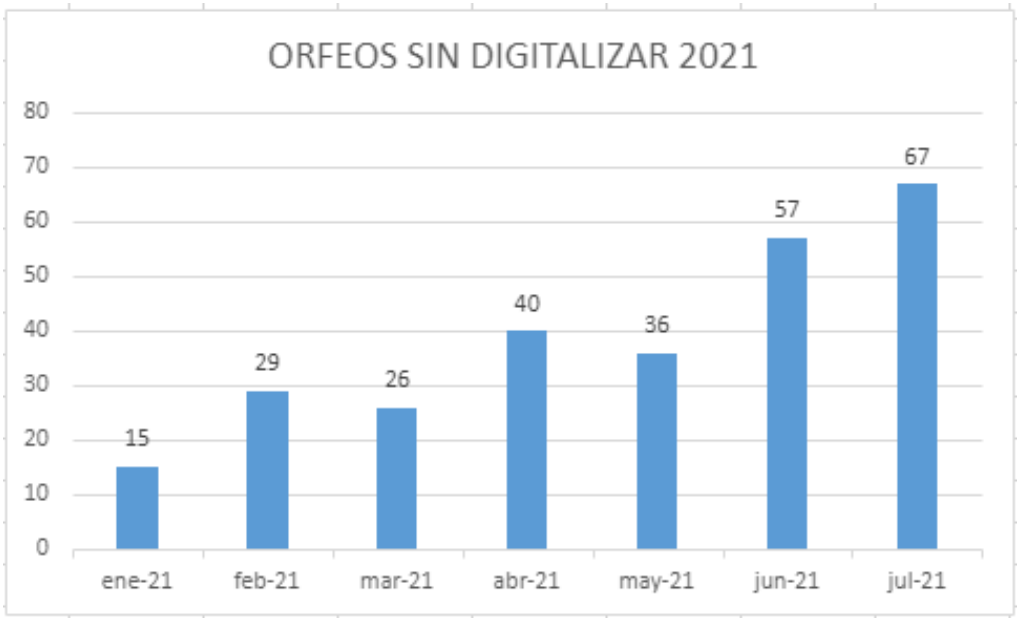
6.7. SEGUIMIENTO A LOS RADICADOS DE SISTEMA DE INFORMACIÓN ORFEO SIN DIGITALIZAR EN EL PERIODO DE ENERO A JULIO 2021.

6.7.1. Radicados de ORFEO sin digitalizar.

Se observan 270 radicados de ORFEO sin digitalizar en el periodo de enero a julio 2021, incumpliendo la *"Política de Seguridad del Sistema de Gestión Documental ORFEO*", que indica: "*El sistema de gestión documental, no permite reservar números de ORFEO*".

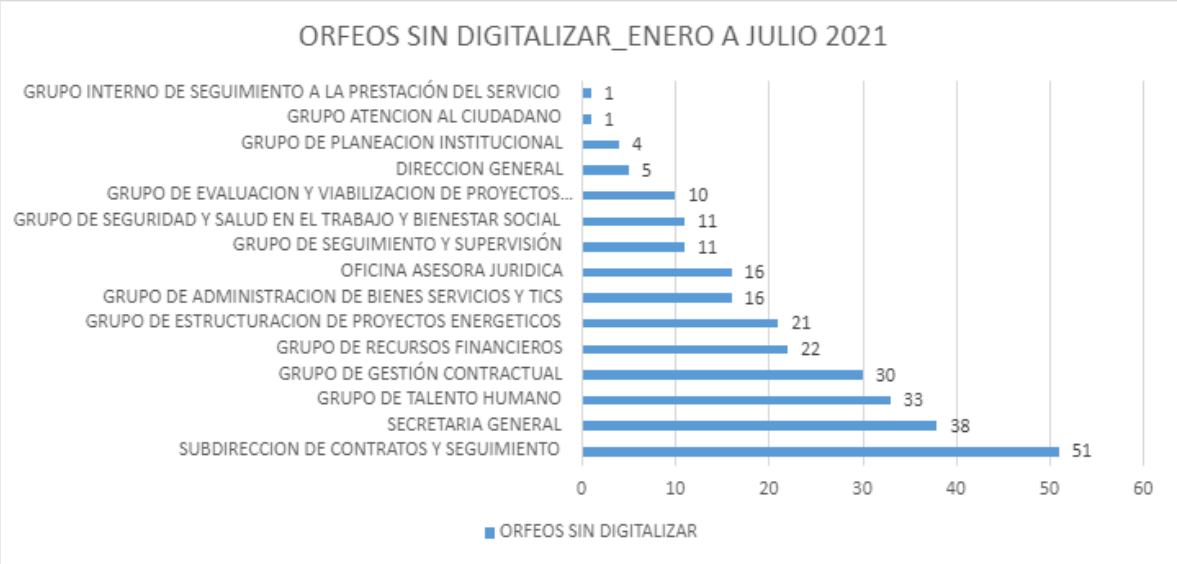
Mediante memorando IPSE-20211330028773 del 20 de agosto 2021, el Grupo de TICs del IPSE, envía el informe de listado de radicados sin digitalización por dependencia, con el siguiente balance:

- El número total de ORFEOS sin digitalizar en el periodo de enero a julio de 2021 es de 270, con la siguiente distribución mensual.



Distribución mensual de ORFEOS sin digitalizar 2021.
Fuente: IPSE-20211330028773

- Y la distribución de ORFEOS sin digitalizar por dependencia es:



Distribución por dependencia de ORFEOS sin digitalizar 2021.
Fuente: IPSE-20211330028773

Incumpliendo la *Política de Seguridad del Sistema de Gestión Documental ORFEO*", *"El sistema de gestión documental, no permite reservar números de ORFEO*", resolución 20171300002585 del 13 de septiembre 2017, página 44, numeral nueve.

Recomendación.
Se debe coordinar con los procesos de Gestión Documental, Grupo de Tecnologías y Sistema de Información, y demás actores de valor del sistema ORFEO para analizar los eventos de ORFEOS sin Digitalizar identificados en la auditoria TI, con el objetivo de mejorar los procesos, el sistema de información, herramienta tecnológica y políticas de seguridad de la información. Se recomienda crear un módulo automático en el sistema ORFEO del IPSE que archive los números de radicado que no se hayan digitalizado en 30 días (Por ejemplo).

6.8. SEGUIMIENTO AL SISTEMA DE INFORMACIÓN SGI – SISTEMA GESTION INTEGRAL

6.8.1. El Sistema Gestión Integral SGI del IPSE, no está operativo.

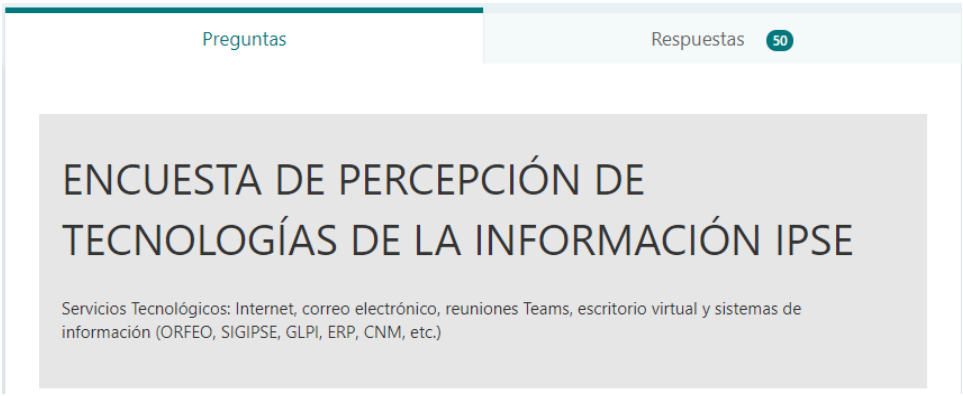
En desarrollo de la auditoria, al realizar verificación de acceso al sistema de información SGI el 29 de noviembre 2021, se observa que el sistema no funciona.

Acceso desde la máquina virtual del IPSE a la dirección:
192.168.111.219/ModeloIPSE/its-gestion/portal/index.php.

Se evidencia la falla del sistema gestión integral SGI del IPSE, que contiene la información de los documentos de procesos y procedimientos, y demás documentos estratégicos para la entidad.

Recomendación. Se recomienda aplicar el procedimiento IPSE-TIC-04 “Soporte y mantenimiento hardware y software” del sistema de gestión integral SGI del IPSE, que inicia con la actividad “*Planear mantenimiento para la vigencia*”. Que incluya el seguimiento y mantenimiento del sistema gestión integral SGI del IPSE, que contiene la información de los documentos de procesos y procedimientos, y demás documentos estratégicos para la entidad.

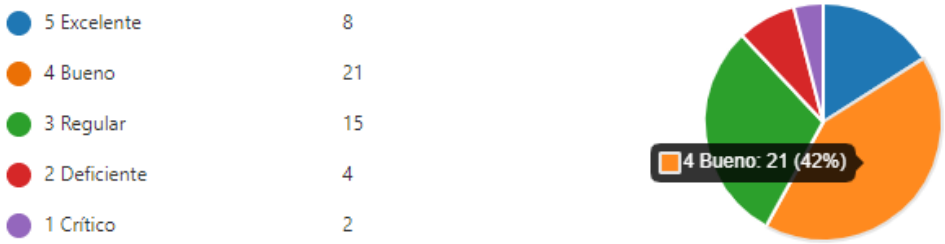
7. RESULTADOS DE LA ENCUESTA DE PERCEPCIÓN TI IPSE 2021



Encuesta realizada en noviembre 2021 al grupo de funcionarios del IPSE, con 50 formularios diligenciados.

PREGUNTA 1.

¿Cuál es su nivel de satisfacción respecto a la CALIDAD y CONTINUIDAD de los Servicios Tecnológicos que presta la entidad, para el desarrollo de sus actividades laborales en el IPSE?

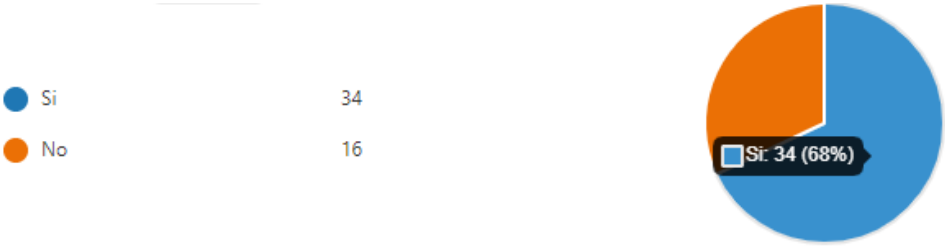


Resultado a la pregunta 1.

Se observa que el 42% de la muestra, indica un nivel de satisfacción a la calidad y continuidad de los servicios tecnológicos como “Bueno”.

PREGUNTA 2.

¿Ha tenido problemas de conexión y acceso al escritorio virtual que haya afectado el desarrollo de sus actividades laborales en el IPSE, durante el periodo 2020-2021?



Resultado a la pregunta 2.

Se observa que el 68% de la muestra, indica que ha tenido problemas de conexión y acceso al escritorio virtual que haya afectado el desarrollo de sus actividades laborales en el IPSE, durante el periodo 2020-2021.

PREGUNTA 3.

¿Cuál es su mayor inconformidad con los servicios de tecnología de la entidad y que propone como solución?

Respuestas:

Falla de acceso a la maquina virtual.
La falta de continuidad y confiabilidad
La interrupción en el servicio y la demora al momento de guardar los documentos.
Intermitencia en el cargue de la máquina y en ocasiones en el Windows
Interrupción del servicio, impedimento para acceder a las plataformas intranet y demora

en guardar los documentos.
Ninguna
Se cae contantemente el servicio y los equipos son obsoletos, actualizar equipos con mejor tecnología y software
El tema de la conexión a la red de internet
El internet de las oficinas es muy lento
Lentitud de acceso a la VPN del CNM (sede calle 82). Ampliación del ancho de banda de la 82.
La demora en brindar inducción y capacitación sobre las herramientas. Propongo que se sensibilice a los procesos de apoyo como éste de TICS que así sea un funcionario, este debe recibir oportunamente la inducción y capacitación porque en el IPSE no hay ingresos masivos de funcionarios.
maquina virtual
es lento el sistema y a veces se cierra sesión
ninguna
Ninguno
hay que mejora el sistema de internet
N/A
No tener licencia para un procesador de documentos PDF profesional, el trabajo requiere manejar muchos documentos PDF y las versiones libres tienen muchas limitantes.
Se han presentado problemas con las máquinas virtuales, pero es muy útil el soporte del office 365, el cual se puede ejecutar desde cualquier computador, el no acceso a la máquina virtual si ha ocasionado problemas con el acceso al ORFEO y a las carpetas del área, adicional la capacidad operativa de los equipos es limitada, si se abren varios Excel en ocasiones colapsa y lo cierra todo.
Equipo Portátil Obsoleto - Adquirir nuevos equipos
el rendimiento de la máquina virtual, se deben aplicar las mejoras tecnológicas que sean suficientes para mejorar el servicio
Creo que la solución es la ampliación de la capacidad del servidor,, aunque creo ya lo están haciendo
NO HAY CONEXIÓN DE LOS COMPUTADORES NI EQUIPOS MÓVILES, LA SOLUCIÓN ES COLOCAR MODE DE INTERNET EN CADA ÁREA DE TRABAJO
El servicio es deficiente y registra continuas fallas. Considero que debe revaluarse los contratos externos de soporte tecnico ya que la seguridad de la información ha sido vulnerada con frecuencia ocasionando inconvenientes en las labores de los funcionarios y contratistas del IPSE
Los equipos están desactualizados, mejorar el hardware y software
Uno es la capacidad para guardar información en la carpeta asignada y algunas veces la indisponibilidad de la carpeta. La solución sería ampliar la capacidad para guardar información.
Se deberán actualizar las herramientas ofimáticas y ampliar los anchos de banda
Acceso a la información de la Página WEB y a la Carpeta del Disco IPSE Público, como solución el oportuno monitoreo en la disponibilidad de los servicios tecnológicos por parte de los responsables de TI en la Entidad, y la comunicación oportuna y adecuada a los usuarios notificando sobre la indisponibilidad presentada a fin de conocer que el acceso no es posible en ese momento y conocer que se debe hacer como usuario

porque hasta el momento en mi permanencia en la Entidad no he visto ese tipo de comunicaciones y sin embargo se ha presentado la indisponibilidad, que no permite reportar a la mesa de ayuda y por el contrario al enviar correo a los contactos de TI no responden, o les responden a algunas personas indicándoles una solución rápida para el acceso cuando debería ser generalizada la respuesta a todos los usuarios.
Ninguna
Diligencia
La asistencia por parte del personal de TICS frente a las problemáticas que se presentan con las tecnologías. Pocas veces hay un apoyo real, efectivo y eficiente. En la mayoría de los casos uno no recibe apoyo.
No hay soporte cuando se trata de temas específicos. Hay desconocimiento de algunas aplicaciones, su uso (a pesar de que hace tiempo están siendo utilizadas en al entidad) y no tienen un soporte.
Los Las maquinas no cuentas con los niveles de tecnología adecuado para realizar trabajo virtual (Carencia de Cámaras y deficiencia en sonidorofonos y somputadorres
Intermitencia en conexiones y lentitud en las mismas.
El orfeo no deberia estar en la maquina virtual
Que el sistema sea mas ágil, mas rápido.
Conectividad eficiente y a la altura de la organización.
La Continuidad
POCA ESTABILIAD EN LA CONEXIÓN
Debilidad en la conexión de internet en las oficinas, se podría mejorar
El Orfeo es una herramienta que no brinda capacidades reales de gestión documental, solo sirve para tener un consecutivo de radicación de documentos, en otras instituciones hacen uso de versiones actualizadas mucho mas poderosas y funcionales, en el IPSE nos quedamos en la versión mas básica; igual que en los sistemas de almacenamiento, en la máquina virtual, en las herramientas de gestión de proyectos tanto de estructuración y viabilización como supervisión y seguimiento, se requiere innovación en el IPSE para disponer de herramientas de generación avanzada, capacitación para su uso y una cultura institucional que motive la competitividad, la transparencia y el logro de los fines institucionales con excelencia, alejados de la mediocridad.
Ninguna
El servicio remoto de la maquina virtual es lento en ocasiones
Velocidad de ejecución de tareas. (Equipos mas robustos que permitan aumentar la velocidad de ejecución)
NINGUNO

PREGUNTA 4

¿En caso de identificar una falla de servicios de internet, máquina virtual y/o sistemas de información del IPSE, la reporta a través de la mesa de ayuda GLPI?

Resultado a la pregunta 4.

Se observa que el 22% de la muestra, indica que “Si” reporta la falla a través de la mesa de ayuda GLPI, y un 78% no reporta la falla a la mesa de ayuda.

PREGUNTA 5

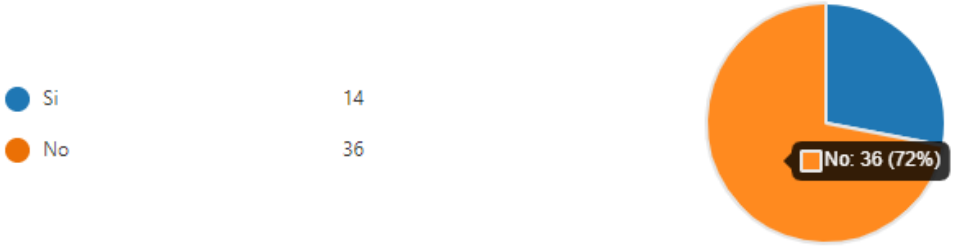
¿Recuerda su usuario y contraseña de ingreso a la mesa de ayuda GLPI?

Resultado a la pregunta 5.

Se observa que el 53% de la muestra, indica que “No” recuerda el usuario contraseña de ingreso a la mesa de ayuda GLPI para reportar fallas de servicio de Tecnologías de la Información del IPSE.

PREGUNTA 6

¿Teniendo en cuenta el modo actual de trabajo en casa, se le consultó sobre la capacidad de internet y equipo de cómputo con el que usted cuenta para desarrollar sus actividades laborales en el IPSE?



Resultado a la pregunta 6.

Se observa que el 72% de la muestra, indica que “No” fue consultado sobre los recursos de internet y equipo de cómputo para desarrollar las actividades laborales en modo de trabajo en casa.

8. CONCUSIONES

8.1. Manual de Gobierno Digital

Se recomienda seguir los lineamientos del Manual de Gobierno Digital[3], que en el módulo de implementar indica “***Una vez la entidad cuente con el PETI y el plan de seguridad y privacidad de la información****, en donde se definieron los proyectos y se establecieron las actividades, responsables, tiempos de ejecución y recursos para la ejecución de la política, ésta debe desarrollar dichas iniciativas o proyectos, aplicando lineamientos que corresponden a los componentes* ***TIC para el Estado y TIC para la Sociedad***”.

Fuente:
https://gobiernodigital.mintic.gov.co/portal/Politica-de-Gobierno-Digital/Manual-de-Gobierno-Digital/

8.2. Modelo de Seguridad y Privacidad de la Información - MSPI

Se recomienda seguir los lineamientos de MinTIC del Modelo de Seguridad y Privacidad de la Información - MSPI, que imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital.

El MSPI lo debe desarrollar el líder o encargado de Seguridad de la Información con el apoyo de toda la estructura organizacional, mediante el Documento Maestro del Modelo de Seguridad y Privacidad de la Información y sus guías de orientación:

Modelo de Seguridad y Privacidad - MSPI
Guía 1 - Metodología de pruebas de efectividad
Guía 2 - Política General MSPI v1
Guía 3 - Procedimiento de Seguridad de la Información
Guía 4 - Roles y responsabilidades
Guía 5 - Gestión Clasificación de Activos

[3] Manual de Gobierno Digital. El Manual de Gobierno Digital es el documento que establece los lineamientos y estándares de los componentes de la política (TIC para el Estado y TIC para la Sociedad) y de los habilitadores transversales (arquitectura, seguridad y privacidad de la información y servicios ciudadanos digitales).

Guía 6 - Gestión Documental
Guía 7 - Gestión de Riesgos
Guía 8 - Controles de Seguridad de la Información
Guía 9 - Indicadores Gestión de Seguridad de la Información
Guía 10 - Continuidad de Negocio
Guía 11 - Análisis de Impacto de Negocio
Guía 12 - Seguridad en la Nube
Guía 13 - Evidencia Digital
Guía 14 - Plan de comunicación, sensibilización, capacitación
Guía 15 - Auditoria
Guía 16 - Evaluación de Desempeño
Guía 17 - Mejora continua
Guía 18 - Lineamientos terminales de áreas financieras de entidades públicas
Guía 19 - Aseguramiento de protocolo IPv4_IPv6
Guía 20 - Transición IPv4_IPv6
Guía 21 - Gestión de Incidentes

Fuente: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

RESOLUCIÓN 00500 DE MARZO 10 DE 2021
"Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad con habilitador de la política de Gobierno Digital"

Fuente:
https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf

8.3. G.ES.06 Guía para la construcción del PETI

Se recomienda seguir la Guía para la construcción del PETI, de MinTIC, realizando la actualizacion correspondiente de todos los documentos tecnicos de la situacion actual AS-IS, la situacion objetivo TO-BE, las brechas con identificadory el mapa de ruta de TI que debe coincidir de forma exacta con el Plan de Inversion de Tecnologias de la Informacion del IPSE.

En el documento *"G.ES.06 Guía para la construcción del PETI"* se presenta la metodología que **las entidades deben seguir** para diseñar e implementar un Plan Estratégico de las Tecnologías de Información PETI. El objetivo de esta guía es orientar a la Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, durante la elaboración de su Plan Estratégico de Tecnologías de la Información.

Fuente: https://mintic.gov.co/arquitecturati/630/w3-article-15031.html

8.4. Lineamientos del modelo de gobierno de tecnologías de la información y del modelo de gobierno de datos del sector minero energético

Se recomienda seguir la RESOLUCIÓN 40199 DE 28 DE JUN 2021 del Ministerio de Minas y Energía, por la cual se adoptan los lineamientos del modelo de gobierno de tecnologías de la información y del modelo de gobierno de datos del sector minero energético.

...Articulo 1. Objeto: *Adoptar los lineamientos del modelo de gobierno de tecnologías de la información y del modelo de gobierno de datos del sector minero energético, entendidos como dominios (componentes) de arquitectura empresarial sectorial, mediante los cuales se brinda directrices para la implementación de esquemas de gobernabilidad de tecnologías de la información y de datos y se adoptan las políticas que permitan alinear los procesos, planes de las instituciones con los del sector.*

Esto, con el fin de gestionar el uso de los datos de toma de decisiones, divulgación de la información, operaciones sectoriales, sistemas de información y articulación con las diferentes estrategias, basados en información, analítica de datos y servicios tecnológicos, cumpliendo con todos los lineamientos de Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia en adelante "MinTIC", y los que se expidan por las autoridades nacionales...

Fuente*:* RESOLUCIÓN 40199 DE 28 DE JUN 2021
https://www.minenergia.gov.co/documents/10180//23517//48979-RESOLUCI%C3%93N+40199+DEL+28-6-2021.pdf

8.5. Mantenimiento de hardware y software del IPSE

Se recomienda aplicar el procedimiento IPSE-TIC-04 "Soporte y mantenimiento hardware y software" del sistema de gestión integral SGI del IPSE, que inicia con la actividad de planear mantenimiento para la vigencia, y seguir los lineamientos de la norma ANSI / TIA 942 para centros de datos.

Fuente:
Sistema de Gestion Integral SGI, procedimiento
https://tiaonline.org/products-and-services/tia942certification/ansi-tia-942-standard/

8.6. Revisión y actualización del proceso y procedimientos de Gestión de TICs

Se recomienda realizar la revisión del proceso IPSE-TIC-C01 de Gestión de TICS y sus procedimientos para actualización a la situación actual de IPSE:

- IPSE-TIC-P02 Procedimiento seguridad y privacidad de la información.
- IPSE-TIC-P03 Procedimiento de innovación tecnológica.
- IPSE-TIC-P03 Procedimiento de soporte y mantenimiento hardware y software.

Y realizar el cambio de procedimiento IPSE-TIC-P02 "Procedimiento de Privacidad y Seguridad de la Información - Backup's de información y transferencia", en el módulo de

Backus de información.

8.6. Mesa de ayuda GLPI

Se recomienda aplicar el lineamiento **LI.ST.09. Mesa de ayuda o de servicios**, asociado al ámbito AM.ST.03. Soporte de los Servicios Tecnológicos, de MinTIC, el cual está contenido en los documentos entregados mediante radicado 20211340021263 del grupo de TIC, en la carpeta ST (Servicios Tecnológicos).

Se recomienda actualizar el procedimiento IPSE-TIC-P03 Procedimiento de soporte y mantenimiento hardware y software, al lineamiento **LI.ST.09. Mesa de ayuda o de servicios.**

Se recomienda hacer actividad de Uso y Apropiación de la herramienta Mesa de Ayuda GLPI para que los usuarios del IPSE reporten las fallas del sistema, quedando el registro de la falla, de la solución, el tiempo de respuesta y la base de conocimiento para efectuar las mejoras en Tecnologías de la Información de la Entidad. En la encuesta de percepción se observa que el 22% de la muestra, indica que “Si” reporta la falla a través de la mesa de ayuda GLPI, y un 78% no reporta la falla a la mesa de ayuda.

Como mesa de Servicio o Ayuda se entiende el conjunto de recursos técnicos y humanos, que se articulan para gestionar y solucionar las posibles incidencias o fallas de manera integral, junto con la atención de requerimientos relacionados con las TICs.

Este procedimiento establece varios controles durante su ejecución para asegurar la prestación del servicio en forma oportuna, eficaz y efectiva, a través del cumplimiento de términos, seguimiento a la calidad y respuesta, satisfacción de usuarios, disponibilidad y medición de indicadores de servicio entre otras.

Fuente:
Radicado 20211340021263, carpeta ST.
Mesa_Servicios_LI.ST.09_V1.0.DOCX – Mesa de Servicios

INFORME FINAL

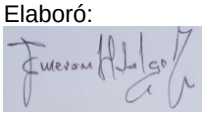
AUDITORÍA INTERNA A LOS PROCESOS DE LAS TECNOLOGÍAS DE LA INFORMACIÓNY COMUNICACIONES – TIC IPSE 2021

Atentamente,

SAUL ALBERTO ROMERO PIÑEROS
Firmado digitalmente por SAUL ALBERTO ROMERO PIÑEROS
Fecha: 2021.12.10 14:02:33 -05'00'

SAUL ALBERTO ROMERO PIÑEROS
Jefe Oficina de Control Interno
Supervisor Contrato IPSE 084-2021

Elaboró:



EMERSON GIOVANI HIDALGO MARTIN
Contrato IPSE 084-2021

Revisó

WILLIAM HUMBERTO ROA BARRAGAN
Profesional Especializado – Control Interno

BELEN ETELVINA CACERES FORERO
Profesional Especializado – Control Interno

Versión 1
7 diciembre 2021