CEDELCA
Centrales Eléctricas del Cauca S.A E.S.P

Radicado No. CI-2023-0235
Fecha Radicado 2023-05-30 11:45:05
Recibido: LUZ ENITH FERNANDEZ GOMEZ
Destino: DIANA LORENA ASTUDILLO QUIRA
Dependencia: SUBGERENCIA FINANCIERA Y ADMINISTRATIVA - 150
Remitente: LUZ ENITH FERNANDEZ GOMEZ
Folios: 1
Anexos: 0 DOC

INFORME FINAL DE AUDITORÍA INTERNA AL SUBPROCESO DE INFORMÁTICA Y COMUNICACIONES

1. INFORMACIÓN GENERAL

Proceso Auditado: Gestión Financiera y Administrativa Subproceso: Informática y Comunicaciones	Dependencia: Oficina Informática y Comunicaciones
Equipo de trabajo: Fernando Andrés Estrada Romero	Cargo: Profesional Universitario II
Fecha: Del 05/05/2023 al 24/05/2023	Duración (total días auditor): 13 días hábiles

2. OBJETIVOS

OBJETIVO GENERAL:

Realizar una evaluación objetiva, ordenada e independiente del proceso de Informática y comunicaciones de conformidad con los requisitos normativos legales vigentes aplicables al mismo, y los establecidos internamente, con el fin de emitir concepto de evaluación acerca de los aspectos más importantes sobre la gestión del proceso basados en evidencias objetivas, facilitando los resultados obtenidos a disposición de la administración para que sean considerados en la toma de decisiones, agregando valor a través de las auditorías.

OBJETIVOS ESPECÍFICOS:

- Verificar el cumplimiento de los requisitos legales vigentes aplicables al proceso de Informática y Comunicaciones, y los establecidos internamente en la operación que se ejecuta dentro del mismo.
- Verificar el cumplimiento de los objetivos estratégicos trazables al proceso de Informática y Comunicaciones, de acuerdo con los indicadores de desempeño establecidos.
- Verificar el cumplimiento de la aplicación de los controles formulados a los riesgos del proceso de Informática y Comunicaciones; y evaluar la efectividad de los mismos.

- Verificar el grado de cumplimiento del proceso de mejora continua, a través de los resultados de ejecución de los Planes de Mejoramiento producto de las Auditorías Internas y Externas al proceso de Informática y Comunicaciones.
- Verificar la idoneidad, la adecuación, y la eficacia del sistema de gestión establecido e implementado por Centrales Eléctricas del Cauca S.A. E.S.P., frente al proceso auditado que permita identificar las oportunidades para la mejora del sistema y de su desempeño.
- Proporcionar a la administración información para la toma de decisiones sobre la mejora del sistema de gestión.

3. ALCANCE

La Auditoría Interna se aplicará mediante evaluación del diseño y efectividad del Sistema de Control Interno del proceso de Informática y Comunicaciones en Centrales Eléctricas del Cauca S.A. E.S.P. y al seguimiento de su gestión durante la vigencia 2023, para verificar en forma selectiva el cumplimiento de los requisitos legales y reglamentarios, con corte a 30 de abril de 2023.

4. CRITERIOS DE AUDITORIA

INTERNOS:

- ESTATUTOS
- Resolución No. 04 (4 de enero de 2021) "Por medio de la cual se adopta el Plan Estratégico 2021 - 2025 de CENTRALES ELÉCTRICAS DEL CAUCA S.A. E.S.P."
- Directiva Gerencial No.003 del 31 de enero de 2023 "Adopción del Plan de Acción de Centrales Eléctricas del Cauca – CEDELCA S.A. E.S.P. para la vigencia 2023.
- Directiva Gerencial No.005 del 31 de enero de 2023 "Adopción de Planes Operativos por procesos de Centrales Eléctricas del Cauca – CEDELCA S.A. E.S.P. para la vigencia 2023.
- Directiva Gerencial No. 19 del 28 de diciembre de 2022 "Adopción y reglamentación del Sistema Integrado de Gestión de Centrales Eléctricas del Cauca S.A. Empresa de Servicios Públicos – CEDELCA S.A. E.S.P.

PRGFA14- Requerimiento de soporte de software, hardware y Asesoría para Usuarios
PRGFA15- Generación y Restauración de backups
PRGFA16- Administración de cuentas de usuarios

PRGFA17- Mantenimiento preventivo de equipos.
PRGFA18- Baja de equipos.
PRGFA19- Administración del sitio web.
PRGFA20- Administración cámara de seguridad.
PRGFA21- Administración redes sociales.

- Directiva Gerencial 009-2022 "Adopción del Plan Estratégico de la Información y las Comunicaciones PETI 2022-2025, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y el Plan Estratégico de la Información y Ciberseguridad de CENTRALES ELÉCTRICAS DEL CAUCA S.A. E.S.P.
- Resolución No.011 del 31/08/2013 "Por medio de la cual se adopta el manual interno de políticas de tratamiento de la información personal de Centrales Eléctricas del Cauca - Cedelca S.A E.S.P.".
- Resolución No.22 del 05/12/2019, por medio de la cual se adopta la política general de seguridad de la información de Centrales Eléctricas del Cauca CEDELCA SA ESP.
- Resolución No. 016 (11 de junio del 2020) "Por medio del cual se adopta la Política y procedimiento de tratamiento de datos de Centrales Eléctricas del Cauca - Cedelca S.A E.S.P." - ANEXO No.1
- Reglamento Interno de Trabajo Centrales Eléctricas del Cauca – Cédela S.A E.S.P. de enero de 2017.

- Directiva Gerencial No. 16 del 29 de noviembre de 2022 "Actualización del Manual Específico de Funciones y Competencias Laborales de la Empresa Centrales Eléctricas del Cauca S.A.
- Demás reglamentación interna aplicable al proceso auditado.

EXTERNAS:

- Artículo 365 de la Constitución Política de Colombia
- Ley 142 de 1994 "Por la cual se establece el régimen de los servicios públicos domiciliarios y se dictan otras disposiciones".
- Decreto 2663 de 1950, Código Sustantivo de Trabajo

- Ley 1712 de 2014, Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Decreto 1494 de 2015, "Por el cual se corrigen yerros en la Ley 1712 de 2014".
- Decreto 103 de 2015, por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- Ley 1755 del 30 de junio de 2015 - Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- RESOLUCIÓN N° 001519 del 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"
  - Anexo 01: directrices de accesibilidad web
  - Anexo 02: estándares de publicación y divulgación de contenidos e información
  - Anexo 03: condiciones mínimas técnicas y de seguridad digital
  - Anexo 04: condiciones mínimas de publicación de datos abiertos
- Ley 2195 de 2022, Por medio de la cual se adoptan medidas en materia de transparencia, prevención y lucha contra la corrupción y se dictan otras disposiciones.
- Demás normatividad aplicable al proceso auditado de acuerdo con los requisitos internos y externos (legales, reglamentarios).

5. EQUIPO AUDITOR

Auditor Líder: Olga Lorena Díaz Chagüendo	Cargo: Jefe de Oficina Control Interno y de Gestión
Auditor de Apoyo: Luz Enith Fernández Gómez Boomer Calvache Riascos	Cargo: Profesional Universitario II Oficina Control Interno y de Gestión Contratista de Apoyo Oficina Control Interno y de Gestión

6. ACTIVIDADES DESARROLLADAS

- Socialización el día 31/01/2023 a los líderes de proceso del PAAI 2023 formulado desde la OCI para su conocimiento de acuerdo con el MANUAL DEL SISTEMA DE CONTROL INTERNO aprobado mediante Directiva de Gerencia No.008 del 04/06/2013 y vigente a la fecha, el cual establece: "ARTÍCULO SÉPTIMO: PROGRAMA DE AUDITORIAS. La Coordinación de

Control Interno o quien haga sus veces, elaborará el calendario anual de auditorías en el cual se describen las auditorías a realizar durante la respectiva vigencia y la periodicidad con que se realizan. Cronograma que deberá socializarse con los coordinadores de las dependencias de la empresa, y los responsables de la información que se necesite para el desarrollo de las auditorias programadas.".

- Notificación del Plan de Auditoría Interna al proceso de Gestión Financiera y Administrativa subproceso Informática y Comunicaciones a la Doctora Diana Lorena Astudillo Quira Subgerente Financiero y Administrativo y Fernando Andrés Estrada Romero Profesional Universitario II Informática y Comunicaciones, según oficio con radicado No. CI-2023-0187, enviado mediante correo electrónico del 08/05/2023.
- Reunión de Apertura el día 05/05/2023, 9:30 a.m, en la oficina de la Subgerencia Administrativa y Financiera en presencia de la Dra: Diana Lorena Astudillo Quira y Fernando Andrés Estrada Romero, Profesional Universitario II.
- Se inicia trabajo de campo el 05/05/2023.
- Se solicita información de muestra para análisis, revisión y recopilación documental de evidencias mediante oficio CI-2023-0191 de fecha 08/05/2023 el cual fue remitido mediante correo electrónico de la misma fecha.
- Se Notifica Informe Preliminar el día 24/05/2023.
- El Auditado no presenta contradicción al Informe Preliminar.
- Se notifica informe Final el día 30-05-2023.

7. HALLAZGOS IDENTIFICADOS

N	Descripción de los Hallazgos
1	**HALLAZGO ADMINISTRATIVO No.1:** Se evidencia falencias en el seguimiento al Plan Estratégico de Tecnologías de la Información y las Comunicaciones – PETI 2022-2025, Plan de Seguridad y Privacidad de la Información, situación que no ha permitido identificar las desviaciones en su implementación que permitan a la empresa tomar decisiones de ajuste, en el caso de ser necesario, o gestionar los recursos de tecnología de la información y las comunicaciones como un factor estratégico generador de valor para CEDELCA S.A. E.S.P, y de esta forma mitigar los riesgos potenciales de incumplimiento que pueden afectar el alcance de los objetivos propuestos en dichos planes. **EVIDENCIA:**

Se solicito información a la Subgerencia Financiera y Administrativa y Oficina de Informática y Comunicaciones para análisis, revisión y recopilación documental mediante oficio No. CI 2023-0191 de fecha 08-05-2023, en el cual se requiere lo siguiente:

1. Plan Estratégico de Tecnologías de la Información y las Comunicaciones – PETI 2022-2025, y su seguimiento con corte a 31/03/2023, allegando evidencia de ejecución.

3. Plan de Seguridad y Privacidad de la Información vigencia 2023, y su seguimiento con corte a 31/03/2023, allegando evidencia de ejecución.

Frente al cual mediante oficio No.CI-2023-0196 de fecha 09-05-2023 se recibe respuesta emitida por el profesional II de la Oficina de Informática y Comunicaciones, donde se indica lo siguiente:

"En atención a la solicitud de información realizada en el marco de la auditoría interna al subproceso Gestión Informática y Comunicaciones, me permito remitir la siguiente información:

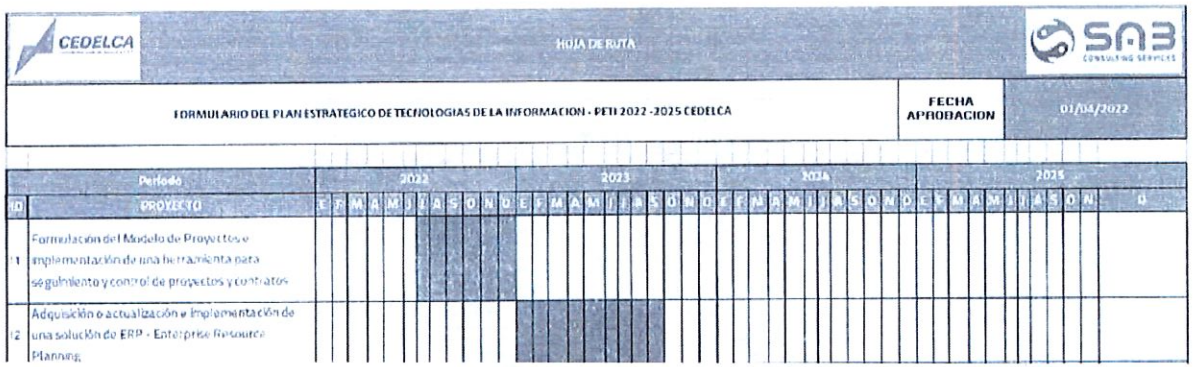
1. Plan Estratégico de Tecnologías de la Información y las Comunicaciones - PETI 2022-2025, y su seguimiento con corte a 31/03/2023
3. Plan de Seguridad y Privacidad de la Información vigencia 2023, y su seguimiento con corte a 31/03/2023"

Se revisa el Plan Estratégico de Tecnologías de la Información y las Comunicaciones – PETI 2022-2025, Plan de Seguridad y Privacidad de la Información en los cuales se evidencian metas establecidas para la vigencia 2022 y primer trimestre de 2023, **sin ejecución a la fecha y/o el seguimiento comunicado a la Gerencia donde se registren las desviaciones** en su implementación que permitan a la empresa tomar decisiones de ajuste, en el caso de ser necesario, o gestionar los recursos de tecnología de la información y las comunicaciones como un factor estratégico generador de valor para CEDELCA S.A. E.S.P, y de esta forma mitigar los riesgos potenciales de incumplimiento que pueden afectar el alcance de los objetivos propuestos, así:

1. En el Plan Estratégico de Tecnologías de la Información y las Comunicaciones – PETI 2022-2025, se evidencia un mapa de ruta, el cual contiene los proyectos priorizados y el cronograma en el cual serán ejecutados, para el caso puntual se analizan los proyectos priorizados para la vigencia 2022 y primer trimestre de 2023, así:

10. MAPA DE RUTA

La hoja de ruta propuesta se plantea acorde con la priorización de los proyectos, basado en los Impactos en la mejora de la operación de CEDELCA y el cumplimiento de objetivos estratégicos. Según el impacto se propone la fase de tiempo recomendada para implementar los proyectos:



Fuente: PETI - Pagina 88

Metas frente a las cuales no se hace referencia en el seguimiento facilitado por la Oficina de Informática y Comunicaciones, como se muestra en la siguiente imagen, dejando como evidencia las falencias en el seguimiento realizado durante la presente vigencia y la ausencia de los respectivos seguimientos para la vigencia 2022, situación que no permitió a la Gerencia tomar decisiones a tiempo frente a las desviaciones presentadas, generando incumplimiento de dichas metas a la fecha.

DESARROLLO

Capacidad	Descripción	Roles	Fase	Avance trimestre I 2023
Gestionar las necesidades del negocio	Habilidad para desarrollar e implementar proyectos de TI como apalancadoras para el desarrollo de los procesos misionales y de apoyo en CEDELCA con el fin de cumplir los objetivos empresariales.	**Coordinador TI Gestor Infraestructura Tecnológica Gestor de proyectos**	INICIAL (2022 - 2023)	0%
Gestionar los activos de TI	Los activos de TI deben ser gestionados mediante el uso de recursos y herramientas adecuados utilizando mejores prácticas como ITIL	**Coordinador Gestor de Mesa de Servicio Gestor Infraestructura Tecnológica**	INICIAL (2022 - 2023)	0%
Gestionar la mesa de servicio	Habilidad para gestionar los recursos TI y servicios TI garantizando la continuidad de la operación de CEDELCA por medio de la administración, mantenimiento y control de la infraestructura y equipos necesarios.	**Coordinador Gestor de Mesa de Servicio Gestor Infraestructura Tecnológica**	INICIAL (2022 - 2023)	70% A través de los contratos licenciamientos y mantenimiento
Gestionar el uso y apropiación de TI	Se debe garantizar que los proyectos, sistemas, servicios y demás componentes de TI son apropiados por la entidad.	**Coordinador Gestor Uso y Apropiación**	INTERMEDIO (2023 - 2024)	0%
Gestionar el gobierno de TI	La entidad debe gestionar y mantener una capacidad para gobernar TI, esto corresponde a garantizar que el presente modelo se cumpla y se mejore continuamente. Se deben seguir las mejores prácticas como COBIT	**Coordinador Gestor Uso y Apropiación**	INTERMEDIO (2023 - 2024)	0%
Gestionar la arquitectura empresarial	Habilidad para crear acciones que permitan monitorear, medir y controlar la alineación existente entre la planeación estratégica, los procesos, la información, las aplicaciones y la tecnología dentro de CEDELCA, desde un punto de vista holístico, sinérgico y transversal.	**Coordinador Gestor Uso y Apropiación Gestor de proyectos**	INICIAL (2022 - 2023)	0%
Gestionar la analítica institucional	Habilidad para implementar técnicas y herramientas para el procesamiento, manejo y organización de los datos producidos en CEDELCA.	**Coordinador Gestor de proyectos**	INICIAL (2022 - 2023)	0%
Gestionar las políticas de seguridad	Habilidad para desarrollar e implementar políticas de seguridad de la información que permita proteger los activos de información de CEDELCA	**Coordinador Gestor Uso y Apropiación Gestor de proyectos Gestor Seguridad y Privacidad de la Información**	INICIAL (2022 - 2023)	0%
Gestionar el plan de seguridad de la información	Gestionar el plan de seguridad de la información para reducir posibles riesgos asociados y para dar cumplimiento normativo.	**Coordinador Gestor Uso y Apropiación Gestor Seguridad y Privacidad de la Información**	INICIAL (2022 - 2023)	0%

2. En el Plan de Seguridad y Privacidad de la Información, se evidencian las actividades y la fecha estimada en la cual serán ejecutadas, para el caso puntual se analizan las actividades programadas para la vigencia 2022 y primer trimestre de 2023, así:

ACTIVIDADES PARA EL AÑO 2022

No.	Actividad	Fecha fin Estimada	Producto o entregable
1	**PLANEACIÓN SGSI**		
1.1	Definir Manual de Políticas de Seguridad y Privacidad de la Información en sus lineamientos basado en la norma ISO 27001:2013.	II Semestre 2022	Manual de Políticas de Seguridad y Privacidad de la Información
1.2	Definir roles y responsabilidades específicos respecto a la seguridad de la información. Estableciendo el Comité de Seguridad de la Información.	II Semestre 2022	Manual Roles y Responsabilidades Seguridad de la Información
1.3	Elaborar, aprobar y publicar Circular para adopción de la Política de Seguridad y Privacidad de la Información	II semestre 2022	Circular Reglamentaria Políticas de Seguridad y Privacidad de la Información
2	**AUTODIAGNOSTICO MSPI**		
2.1	Realizar Autodiagnóstico Modelo de Seguridad y Privacidad de la Información – MSPI. Esto es Sistema de gestión de seguridad de la información, sistema de gestión de ciberseguridad y sistema de gestión de continuidad de negocio.	I Trimestre 2022	Informe Autodiagnóstico diligenciado
2.2	Establecer el Plan Estratégico de Seguridad de la Información PESI basado en los Análisis de Brecha o GAP Análisis y la identificación de riesgos digitales.	I Trimestre 2022	Informe PESI
3	**IMPLEMENTACIÓN DEL SGSI**		
3.1	Documentar los procedimientos de operación de tecnología que se realizan frente a la Seguridad de la Información y Ciberseguridad a través de la elaboración o actualización de los siguientes documentos del SGSI: 1. Diseño metodología Gestión de Activos de la Información (matriz clasificación de activos de información). 2. Diseño procedimiento Dar de baja un software. 3. Diseño procedimiento Gestión de capacidad. 4. Diseño procedimiento Gestión de configuración. 5. Diseño procedimiento Gestión de evidencia digital. 6. Diseño procedimiento Gestión de Proveedores.	II Semestre 2022	Procedimientos, formatos y herramientas.

Fuente: Plan de Seguridad y Privacidad de la Información - Pagina 17

	7. Diseño procedimiento Gestión de Incidentes de Seguridad de la Información. 8. Diseño procedimiento Gestión de Vulnerabilidades. 9. Diseño procedimiento intercambio seguro. 10. Diseño procedimiento Propiedad intelectual. 11. Diseño procedimiento Borrador seguro. 12. Diseño procedimiento Gestión de Cambios. 13. Diseño procedimiento Procedimientos de copias de respaldo. 14. Diseño procedimiento cifrado de información. 15. Diseño de metodología de Requerimiento de accesos usuarios. Ciclo de Vida de Usuarios (CVU). Procedimiento Control de Acceso. 16. Metodología Gestión de riesgos de seguridad de la información y ciberseguridad. 17. Documento Adquisición, Desarrollo y Mantenimiento de Sistemas.		
3.2	Elaborar Instructivo Clasificación de activos de información.	II Trimestre 2023	Instructivo y Herramienta Excel de Clasificación activos de información
3.3	Aplicación de Auditorias a Proveedores verificando cumplimiento con Políticas de Seguridad de la Información de Cedelca.	III Trimestre 2023	Soporte de Auditorias realizadas a provedores sobre Seguridad de la Informacion.
4	**OPERACION DEL SGSI**		
4.1	Ejecución de pruebas de análisis de vulnerabilidades informáticas sobre Infraestructura tecnológica	I Trimestre 2022	Informe de Pruebas análisis de vulnerabilidades
4.2	Realizar Ejercicio de clasificación de Activos en todos los procesos de CEDELCA.	II Semestre 2022	Matrices de Clasificación de Activos de Información.
4.3	Implementación de procedimientos de buenas prácticas en gestión de TI realizando uso y apropiación.	II Semestre 2023	Evaluación de Métricas en los procesos de TI
4.4	Levantamiento de riesgos digitales en todos los procesos.	I Trimestre 2022	Matrices de Riesgos Digitales.
5	**PLAN DE SENSIBILIZACIÓN SEGURIDAD DE LA INFORMACIÓN**		
5.1	Realizar campaña de concientización en temas de seguridad de la información a las directivas de Cedelca.	II Trimestre 2022	Reunión Gerencial Seguridad de la Información
5.2	Socializar las Políticas de Seguridad y Privacidad de la Información a todos los funcionarios y contratistas.	II Trimestre 2022	Evidencias de Socialización.
6	**GESTION DE LA CONTINUIDAD DEL NEGOCIO**		
6.1	Diseño y ejecución de Análisis de Impacto al Negocio (BIA).	III Trimestre 2023	Informes BIA
6.2	Diseño Procedimientos Gestión de Crisis y respuesta a incidentes.	III Trimestre 2023	Procedimiento documentado.
6.3	Diseño de Plan de Recuperación de Desastres Tecnológico	III Trimestre 2023	Documentos de Diseño DRP

Fuente: Plan de Seguridad y Privacidad de la Información - Pagina 18

ACTIVIDADES PARA EL AÑO 2023

No.	Actividad	Fecha fin Estimada	Producto o entregable
1	**PLANEACIÓN SGSI**		
1.1	Socializar el Manual de Políticas de Seguridad y Privacidad de la Información actualizado	I Trimestre 2023	Manual de Políticas de Seguridad y Privacidad de la Información aprobado
1.2	Se establecerán las políticas adicionales de seguridad de la información y ciberseguridad basado en la norma ISO 27001:2013. Se realizará **una identificación de riesgos digitales** para una estrategia de aseguramiento de TI adecuada y una gestión de servicios que garanticen una adecuada planificación, entrega y apoyo de las capacidades de TI, dando soporte a las funciones de negocio, basados en normas aceptadas por la industria (como ITIL y COBIT 5)	II Trimestre 2023	Uso y apropiación de las políticas y procedimientos de seguridad y privacidad de la información.
2	**ACTIVOS DE INFORMACIÓN**		
2.1	Realizar el inventario y clasificación de los activos software, hardware y servicios. Fase I	I Trimestre 2023	Matriz Inventario de Activos de información software, hardware y servicios
2.2	Realizar el inventario y clasificación de activos de información en los procesos. Fase I	I Trimestre 2023	Matriz inventario de Activos de Información
3	**OPERACIÓN DEL MSPI**		
3.1	Realizar valoración inicial de los niveles de madurez en los controles establecidos en las herramientas de gestión de riesgos digitales. Fase I.	II Trimestre 2023	GAP análisis actualizado en herramientas de gestión de riesgos digitales. Matriz SOA
3.2	Realizar actualización de los niveles de madurez en los controles establecidos en las herramientas de gestión de riesgos digitales. Fase II.	III Trimestre 2023	GAP análisis actualizado en herramientas de gestión de riesgos digitales. Matriz SOA
4.	**ESTABLECER PLAN DE TRATAMIENTO DE RIESGOS**		
4.1	Actualización de riesgos digitales en todos los procesos y su plan de tratamiento.	I Trimestre 2024	Matriz de riesgos digitales de todos los procesos en las herramientas de

Fuente: Plan de Seguridad y Privacidad de la Información - Pagina 19

Metas frente a las cuales no se evidencia avance en el seguimiento facilitado por la Oficina de Informática y Comunicaciones, como se muestra en la siguiente imagen, como tampoco se generan las alertas u observaciones necesarias a la Gerencia frente al particular, dejando como evidencia las falencias en el seguimiento realizado durante la presente vigencia y la ausencia de los respectivos seguimientos para la vigencia 2022, situación que no permitió tomar decisiones a tiempo frente a las desviaciones presentadas, generando incumplimiento de dichas metas, así:

DESARROLLO

No.	Actividad	Fecha fin Estimada	Producto o entregable	Avance trimestre I 2023
1	**1 PLANEACIÓN SGSI**			
1.1	Socializar el Manual de Políticas de Seguridad y Privacidad de la Información actualizado	I Trimestre 2023	Manual de Políticas de Seguridad y Privacidad de la Información aprobado	0%
1.2	Se establecerán las políticas adicionales de seguridad de la información y ciberseguridad basado en la norma ISO 27001:2013. Se realizará una identificación de riesgos digitales para una estrategia de aseguramiento de TI adecuada y una gestión de servicios que garanticen una adecuada planificación, entrega y apoyo de las capacidades de TI, dando soporte a las funciones de negocio, basados en normas aceptadas por la industria (como ITIL y COBIT 5).	II Trimestre 2023	Uso y apropiación de las políticas y procedimientos de seguridad y privacidad de la información.	0%
2	**ACTIVOS DE INFORMACIÓN**			
2.1	Realizar el inventario y clasificación de los activos software, hardware y servicios. Fase I	I Trimestre 2023	Matriz inventario de Activos de información software, hardware y servicios	50%
2.2	Realizar el inventario y clasificación de activos de información en los procesos. Fase I	I Trimestre 2023	Matriz inventario de Activos de Información	50%
3	**OPERACIÓN DEL MSPI**			
3.1	Realizar valoración inicial de los niveles de madurez en los controles establecidos en las herramientas de gestión de riesgos digitales. Fase I.	I Trimestre 2023	GAP análisis actualizado en herramientas de gestión de riesgos digitales. Matriz SOA	0%
3.2	Realizar actualización de los niveles de madurez en los controles establecidos en las herramientas de gestión de riesgos digitales. Fase II.	III Trimestre 2023	GAP análisis actualizado en herramientas de gestión de riesgos digitales. Matriz SOA	0%
4	**OPERACIÓN DEL SGSI**			

CEDELCA
Centrales Eléctricas del Cauca S.A E.S.P

4.3	Implementación de procedimientos de buenas prácticas en gestión de TI realizando uso y apropiación.	II Trimestre 2022	Evaluación de Métricas en los procesos de TI	0%
5	**IMPLEMENTACION CONTROLES DEL SGSI**			
5.3	Diseñar estrategias del Plan de Recuperación de Desastres Tecnológico	I Trimestre 2023	Informes de Estrategias a implementar.	0%
5.10	Establecer métodos de autenticación fuerte. - Es el proceso en el cual se verifica la identidad de un cliente, entidad o usuario, en función de uno o varios factores de autenticación y consiste en verificar que el usuario es quien dice ser. Ejemplos de estos métodos son la autenticación de doble factor con token (de software o hardware) o pin a celular.	IV Trimestre 2023	Verificar los mecanismos implementados de cifrado sobre la información confidencial en tránsito y en reposo con el fin de mitigar los riesgos asociados a fuga de información.	0%
6	**GESTION DE LA CONTINUIDAD DEL NEGOCIO**			
6.1	Realización de campañas de sensibilización en seguridad y privacidad de la información. Fase I	I Trimestre 2023	Encuestas y evaluaciones de las charlas de sensibilización.	0%
6.2	Asegurar que se atiendan las recomendaciones generadas en los informes y reportes entregados por los grupos de interés como: Proveedores de seguridad informática sobre amenazas y vulnerabilidades explotadas a nivel nacional o mundial. Monitorear su implementación.	II Trimestre 2023	Evidencias de aplicación de recomendaciones de proveedores de seguridad informática.	0%
6.1	Diseño y ejecución de Análisis de Impacto al Negocio (BIA).	III Trimestre 2022	Informes BIA	0%
6.2	Diseño Procedimientos Gestión de Crisis y respuesta a incidentes.	III Trimestre 2022	Procedimiento documentado.	0%
6.3	Diseño de Plan de Recuperación de Desastres Tecnológico	III Trimestre 2022	Documentos de Diseño DRP	0%
7	**AUDITORIA AL SGSI**			
7.1	Revisión independiente de la gestión de la seguridad de la información.	IV Trimestre 2023	Informes de hallazgos de Auditoria.	0%
7.2	Auditorías a los controles de gestión técnicos en seguridad de la información y Ciberseguridad. Basada en ITIL.	III Trimestre 2023	Informes de hallazgos y mejoras.	0%

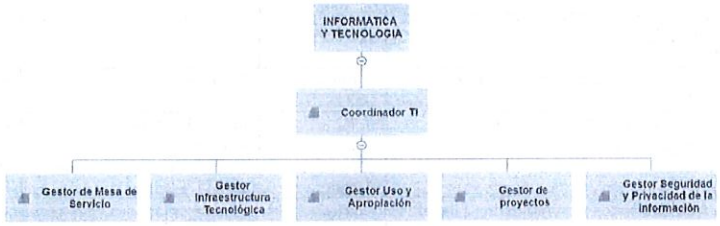
CRITERIO: Incumpliendo en la Directiva Gerencial No. 009 de 2022, "Adopción del Plan Estratégico de la Información y las Comunicaciones PETI 2022-2025, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y el Plan Estratégico de Seguridad de la Información y Ciberseguridad de Centrales Eléctricas del Cauca CEDELCA S.A. E.S.P.

PRIMERO: Adoptar para CENTRALES ELECTRICAS DEL CAUCA CEDELCA S.A E.S.P., Plan Estratégico de la Información y las Comunicaciones PETI 2022 - 2025 de la empresa, plan que hace parte integral de la presenta directiva.

TERCERO: Adoptar el Plan Estratégico de Seguridad de la información y Ciberseguridad de CENTRALES ELECTRICAS DEL CAUCA S.A. E.S.P., con el objeto de establecer los criterios para la identificación, análisis, valoración, acciones y seguimientos a los riesgos potenciales que afecten la confiabilidad, disponibilidad e integridad de la información de CEDELCA S.A. E.S.P., documento que hace parte integral de la presenta directiva

4. RESPONSABLE

El responsable de la Seguridad y Privacidad de la información es el Comité de Seguridad de la Información, que está pendiente de ser establecido en la entidad.



Gráfica 02 - Fuente: Elaboración propia

Un profesional de Tecnologías de información puede asumir varios roles, sin embargo, se considera necesario dar aclaración la importancia de incorporar más profesionales que permitan la distribución de los roles responsabilidades y actividades para una optimización en la gestión de TI en CEDELCA.

2	**HALLAZGO ADMINISTRATIVO No.2:** No se evidencia que CEDELCA S.A. E.S.P. cuente con el diagnostico técnico de los equipos mediante el diligenciamiento del formato FTGAF75-HOJA DE VIDA EQUIPOS donde se determinen las especificaciones técnicas, el estado en el que se encuentran, el mantenimiento aplicado durante el servicio prestado, entre otras cosas, que permitan gestionar su vida útil hasta aplicar el correcto funcionamiento del procedimiento de bajas, ejerciendo el debido control, evaluación y seguimiento de los equipos con los que cuenta la empresa. **EVIDENCIA:** Se solicito información a la Subgerencia Financiera y Administrativa y Oficina de Informática y Comunicaciones para análisis, revisión y recopilación documental mediante oficio No. CI 2023-0191 de fecha 08-05-2023, en el cual se requiere lo siguiente: **g.** Diagnóstico técnico de los equipos determinando la situación en la que se encuentra y documento de justificación de las bajas en los equipos remitidas al almacén para su trámite vigencia 2023. Frente al cual mediante oficio No.CI-2023-0196 de fecha 09-05-2023 se recibe respuesta emitida por el profesional II de la Oficina de Informática y Comunicaciones, donde se indica lo siguiente: CEDELCA Centrales Eléctricas del Cauca S.A E.S.P c. Evidencia de los requerimientos de las dependencias de la empresa para el diseño, adquisición, puesta en marcha y asesoría en los Sistema de Información y herramientas tecnológicas de la empresa vigencia 2023. d. Cronograma de copias de respaldo vigencia 2023. e. Evidencia de los registros de la generación y restauración de backups vigencia 2023. f. Registro de las solicitudes y retiro de usuarios (administrador de cuentas) vigencia 2023. g. A la fecha la oficina de informática y comunicaciones NO ha realizado diagnóstico técnico de los equipos para determinar bajas en la vigencia 2023.

Una vez verificada la información enviada por el profesional II de Informática y Comunicaciones mediante comunicación interna CI-2023-0196, no se evidencia el diagnostico técnico de los equipos mediante el diligenciamiento del formato FTGAF75-HOJA DE VIDA EQUIPOS donde se determinen las especificaciones técnicas, el estado en el que se encuentran, el mantenimiento aplicado durante el servicio prestado, entre otras cosas, que permitan gestionar su vida útil hasta aplicar el correcto funcionamiento del procedimiento de bajas, ejerciendo el debido control, evaluación y seguimiento de los equipos con los que cuenta la empresa a la fecha.

CRITERIO: Incumpliendo lo dispuesto en la Directiva Gerencia N° 19 día 28 de diciembre de 2022, la cual establece el procedimiento **PRGF18 - BAJA DE EQUIPOS**, utilizando la siguiente metodología:

CEDELCA	GESTIÓN FINANCIERA Y ADMINISTRATIVA	PRGFA18
		Versión 03
	BAJA DE EQUIPOS	28/12/2022
		Página 1 de 2

OBJETIVO:	Establecer los lineamientos y actividades para dar de baja los equipos que por su estado de obsolescencia y/o daño físico de hardware o software no cumplan con el objetivo de su adquisición y asignación, por lo que deben ser dados de baja.	**SUBPROCESO REFERENTE:**	TECNOLOGÍA DE LA INFORMACIÓN Y LAS COMUNICACIONES
ALCANCE:	Empieza cuando se recoge el equipo del usuario y lo traslada a la oficina de tecnología de la información y las comunicaciones y finaliza cuando se elabora la baja del equipo, se envía a almacén con la justificación para que ellos dan la disposición final.	**DOCUMENTACIÓN DE REFERENCIA:**	NORMA ISO 27.001

TÉRMINOS Y DEFINICIONES	
BAJA DE EQUIPOS	Acto administrativo que refleja los equipos susceptibles de donación y destrucción, identificando la descripción del equipo que sirve como soporte contable para su retiro.
DIAGNOSTICO TECNICO	Sistema mediante el cual se determinan las necesidades de mantenimiento o reparación de un equipo, comparando sus parámetros de funcionamiento con los establecidos por el fabricante.

DESCRIPCIÓN DE ACTIVIDADES			
PASO	**ACTIVIDADES**	**REGISTROS**	**RESPONSABLE**

1	Se recoge el equipo del usuario y se traslada a la oficina de Tecnología de la Información y las Comunicaciones.		Profesional Universitario II TICs
2	Se elabora el diagnóstico técnico del equipo, donde se determinan la situación en la que se encuentra.	FTFGA 77_Ficha técnica para baja FTFGA 75_Hoja de vida de equipos	Profesional Universitario II TICs
3	Elabora la baja del equipo, se envía a almacén justificación de porque se da de baja el equipo y almacén le da la disposición final.	FTFGA 77_Ficha técnica para baja	Profesional Universitario II TICs

ASPECTOS	ELABORADO POR:	REVISADO POR:	APROBADO POR:
NOMBRE:	EVERGREEN CONSTRUCTORES S.A.S	DIANA LORENA ASTUDILLO QUIRÁ	MARIA BRAVO CUELLAR
CARGO:	CONTRATISTA CONTRATO No. 074 DE 2021	SUBGERENTE FINANCIERO Y ADMINISTRATIVO	GERENTE SUPLENTE

VERSIÓN	DESCRIPCIÓN DEL CAMBIO	FECHA
1	Sin información	Marzo 12 de 2018
2	Sin información	Julio 31 de 2019
3	Se modifica en forma general el contenido del procedimiento, se eliminan las columnas diagrama de flujo y observaciones. Se cambia el tipo de letra de "Tahoma" por "Century Gothic". Se incluye la descripción del cambio y los formatos diseñados	Agosto 09 de 2022

De igual forma desconociendo en el diligenciamiento del formato **FTGAF75-HOJA DE VIDA EQUIPOS**, adoptado mediante Directiva Gerencia N° 19 día 28 de diciembre de 2022 "Adopción y reglamentación del Sistema Integrado de Gestión de CENTRALES ELÉCTRICAS DEL CAUCA S.A. E.S.P.

CEDELCA	HOJA DE VIDA DE EQUIPOS	FTGFA75 Versión 01 28/12/2022 Página 1 de 3

INFORMACIÓN DEL EQUIPO			
ID	TIPO EQUIPO	DEPENDENCIA	NOMBRE RESPONSABLE DE INVENTARIO

INFORMACIÓN DE ADQUISICIÓN		
MARCA DE EQUIPO	MODELO DE EQUIPO	SERIAL DE FABRICA DEL EQUIPO
TIEMPO DE GARANTÍA	PROVEEDOR	FECHA DE ADQUISICIÓN

RELACIÓN DE DOCUMENTOS DE SOPORTE	
DOCUMENTO	UBICACIÓN

HARDWARE Y SOFTWARE					
APLICA		SI		NO	

HARDWARE PARA TIPO MONITOR					
Tipo de monitor		Tamaño de pantalla en pulgadas		Tipo de conector	
Serial de fabrica del equipo		Placa de inventario de CPU asignada al monitor			

HARDWARE PARA TIPO CPU - PORTATIL - AIO - SERVIDOR							
Procesador marca		Modelo		Bits (32 o 64)		Núcleos procesador	
Velocidad procesador		Memoria RAM		Tipo de memoria RAM		Cantidad discos duros	
Tecnología disco duro 1		Capacidad disco 1		Tecnología disco duro 2		Capacidad disco 2	
Lector y/o quemador DVD/CD		Tarjeta video integrada		Tarjeta video independiente		Conectores VGA	

Puertos HDMIa	°a	Puertos displayportª	°a	Puertos USB2ª	°a	Puertos USB3ª	°a
Marca mouseª	°a	Calcomanía mouseª	°a	Señal mouseª	°a	Tipo conector mouseª	°a
Marca tecladoª	°a	Calcomanía tecladoª	°a	Señal tecladoª	°a	Tipo conector tecladoª	°a
Tarjeta de red ethernetª	°a			Tarjeta de red inalámbricaª	°a		
Señal cargadoraª	°a			Placa inventario cargadoraª	°a		
HARDWARE PARA TIPO IMPRESORA - MULTIFUNCIONALª							
Tecnología de impresiónª	°a	Color y / o B-Nª	°a	Tipo (Multifuncional - sólo impresión)ª	°a	Velocidad de Impresión PPMª	°a
Puertos USBª	°a	Puertos ethernetª	°a	Puerto LPTª	°a	Número de bandejasª	°a
Velocidad de escaneo multifuncionalª	°a			Alimentador manual multifuncionalª	°a		
HARDWARE TIPO ESCANERª							
Velocidad de escaneoª	°a	Alimentador automáticoª	°a	Conectores USBª	°a	Conectores ethernetª	°a
ROUTER Y ACCES POINT (AP)ª							
Velocidadª	°a	Modoª	°a	Protocoloª	°a	POEª	°a
Rangoª	°a	Puertos Ethernetª	°a	DHCPª	°a	IPª	°a

CENTRAL PBXª							
Número total de troncalesª	°a			Número de extensionesª	°a	IPª	°a
FIREWALLª							
Puertos RJ-45ª	°a	Puertos RJ-45 WANª	°a	Número de sesionesª	°a	GBPS salida a través del Firewallª	°a
SWITCHESª							
Tecnología de conectividadª	°a	Puertos SFP/SFP+ª	°a	Capacidad de conmutaciónª	°a	Administración basada en webª	°a
Puertos RJ-45ª	°a	Estándares de redª	°a	DHCPª	°a	Tasa de transferenciaª	°a
CONFIGURACIÓN DE REDª							
Nombre red del equipoª	En red (si/ no)ª	Dominio o grupo de trabajo del equipoª		Dirección IPª		Dirección MACª	
°a	°a	°a		°a		°a	
Sistema operativoª	°a		Versiónª	°a		Service packª	°a
SOFTWARE INSTALADOª							
No.ª	Nombreª	Descripciónª	Versiónª	Software libreª		No. Licenciaª	Fecha caducidad licenciaª
°a	°a	°a	°a	°a		°a	°a
°a	°a	°a	°a	°a		°a	°a
°a	°a	°a	°a	°a		°a	°a

ANEXOS Y OBSERVACIONES							
Mantenimiento (PREVENTIVO -P, CORRECTIVO -C)							
Fecha	Tipo (P o C)	Realizado por	Observaciones mantenimiento				
Ubicación actual del equipo							
Fecha	Responsable	Cargo	Piso	Área			
REGISTRO FOTOGRÁFICO							

3	**HALLAZGO ADMINISTRATIVO No.3:** No se evidencia que CEDELCA S.A. E.S.P. cuenta con la implementación de la metodología de administración de riesgo establecida en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, mediante la formulación y/o actualización del Mapa de Riesgos para la vigencia 2023, que permita la mitigación de la materialización de los riesgos que podrían afectar la gestión, incumplimiento con las disposiciones normativas y dificultando el control de evaluación y vigilancia de la OCI delegadas por la administración. **EVIDENCIAS:** Se solicito información a la Subgerencia Financiera y Administrativa y Oficina de Informática y Comunicaciones para análisis, revisión y recopilación documental mediante oficio No. CI 2023-0191 de fecha 08-05-2023, en el cual se requiere lo siguiente: **2.** Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información vigencia 2023, y su seguimiento con corte a 31/03/2023, allegando evidencia de ejecución.

5. Mapa de riesgo del subproceso Gestión Informática y Comunicaciones revisado y actualizado a la vigencia 2023, con las evidencias de la metodología utilizada y los resultados de monitoreo y seguimiento a 31/03/2023, el cual describa sus avances.

Frente al punto numero dos el profesional II de la Oficina de Informática y Comunicaciones remite mediante oficio No.CI-2023-0196 de fecha 09-05-2023 respuesta donde se indica lo siguiente:

"En atención a la solicitud de información realizada en el marco de la auditoría interna al subproceso Gestión Informática y Comunicaciones, me permito remitir la siguiente información:

2. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información vigencia 2023, y su seguimiento con corte a 31/03/2023."

En cuanto a su seguimiento, el profesional manifiesta no contar con dicho elemento de control, como se detalla en la siguiente imagen:

3. ALCANCE

Teniendo en cuenta que el nivel de madurez de implementación del Modelo de Seguridad y Privacidad de la Información en la Entidad está en nivel 1. Inicial, el plan de gestión del riesgo asociado a los activos de información se debe realizar el levantamiento de activos de información, la clasificación, etiquetado y priorización de éstos para poder iniciar con la gestión del riesgo.

Como lo indica el Alcance del documento, la entidad se encuentra en nivel 1, para lo cual en el primer trimestre de la vigencia 2023, se llevó a cabo el levantamiento inicial de los activos con los que cuenta la empresa, actividad que a la fecha todavía continúa ejecutándose.

Una vez analizado el documento, se evidencia que el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información contiene los siguientes aspectos:

TABLA DE CONTENIDO

Así mismo, se evidencia el alcance del mencionado plan, así:

> **3. ALCANCE**
>
> Teniendo en cuenta que el nivel de madurez de implementación del Modelo de Seguridad y Privacidad de la Información en la Entidad está en nivel 1**. Inicial,** el plan de gestión del riesgo asociado a los activos de información se debe realizar el levantamiento de activos de información, la clasificación, etiquetado y priorización de éstos para poder iniciar con la gestión del riesgo.

Lo que permite concluir que dicho documento solamente contiene una metodología de administración de riesgo establecida, **para ser implementada a partir del levantamiento de los activos de información**, clasificando de las 37

amenazas y las 77 vulnerabilidades más comunes identificadas en el texto; cuales de ellas son más probables de materialización en la empresa de acuerdo a la gestión de la información, permitiendo identificar los riesgos y procediendo a la evaluación de los mismos, a través de la probabilidad y el impacto, y con base en el resultado se planifica la acción frente al riesgo para mitigar su materialización, procediendo al monitoreo y seguimiento permanente de las medias de control establecidas. **Procedimiento que no ha sido implementado dado que se considera que la empresa se encuentra en la fase inicial desde la vigencia 2022, fecha en la cual se elabora la metodología expuesta hasta la presente auditoría interna.**

A continuación, se extrae del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información un resumen de la metodología de administración de riesgo planteada como soporte de la conclusión anteriormente manifestada:

Identificación de amenazas

Las amenazas son los peligros externos que buscan afectar la confidencialidad, integridad o disponibilidad de la información, en la siguiente tabla se describen detalladamente las 37 amenazas más comunes asociadas a la afectación de los 3 pilares de la seguridad de la información, las cuales están clasificadas en 7 tipos de amenaza.

Identificación de las Vulnerabilidades:

número consecutivo de la vulnerabilidad. A continuación, se relacionan las 66 vulnerabilidades más comunes asociadas a los tipos de activos enunciados en el párrafo precedente.

Identificación de Riesgos:

Una vez identificadas las amenazas y vulnerabilidades se deben identificar los riesgos basados en los activos de la información, para ello se ha elaborado una tabla que permite la identificación general del riesgo relacionando con el tipo de activo de información, asociando la vulnerabilidad por explotar, la amenaza y la consecuencia del riesgo.

Probabilidad e impacto:

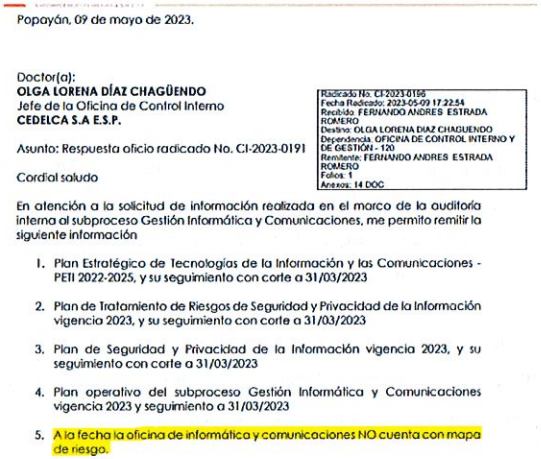
El sistema de evaluación del riesgo está basado en dos variables, la probabilidad y el impacto.

La evaluación del riesgo es la multiplicación de los factores probabilidad e impacto, el resultado se clasifica en el mapa de calor el cual se presenta la siguiente tabla de valor.

Acciones de mitigación frente al riesgo:

Con base en el resultado se planifica la posible acción frente al riesgo:

Frente al punto número cinco el profesional II de la Oficina de Informática y Comunicaciones remite mediante oficio No.CI-2023-0196 de fecha 09-05-2023 respuesta donde se indica lo siguiente:



Popayán, 09 de mayo de 2023.

Doctor(a):
OLGA LORENA DÍAZ CHAGÜENDO
Jefe de la Oficina de Control Interno
CEDELCA S.A E.S.P.

Radicado No. CI-2023-0196
Fecha Radicado: 2023-05-09 17:22:54
Recibido: FERNANDO ANDRES ESTRADA ROMERO
Destino: OLGA LORENA DIAZ CHAGUENDO
Dependencia: OFICINA DE CONTROL INTERNO Y DE GESTIÓN - 120
Remitente: FERNANDO ANDRES ESTRADA ROMERO
Folios: 1
Anexos: 14 DOC

Asunto: Respuesta oficio radicado No. CI-2023-0191

Cordial saludo

En atención a la solicitud de información realizada en el marco de la auditoría interna al subproceso Gestión Informática y Comunicaciones, me permito remitir la siguiente información

1. Plan Estratégico de Tecnologías de la Información y las Comunicaciones - PETI 2022-2025, y su seguimiento con corte a 31/03/2023
2. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información vigencia 2023, y su seguimiento con corte a 31/03/2023
3. Plan de Seguridad y Privacidad de la Información vigencia 2023, y su seguimiento con corte a 31/03/2023
4. Plan operativo del subproceso Gestión Informática y Comunicaciones vigencia 2023 y seguimiento a 31/03/2023
5. A la fecha la oficina de informática y comunicaciones NO cuenta con mapa de riesgo.

En este sentido, No se evidencia que la empresa CEDELCA S.A. E.S.P., cuente con el Mapa de Riesgos del Subproceso Gestión Informática y Comunicaciones revisado y actualizado a la vigencia 2023, con las evidencias de la metodología utilizada y los resultados del monitoreo y seguimiento a 31/03/2023.

CRITERIO:

Incumpliendo en la Directiva Gerencial No. 009 de 2022, "Adopción del Plan Estratégico de la Información y las Comunicaciones PETI 2022-2025, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y el Plan Estratégico de Seguridad de la Información y Ciberseguridad de Centrales Eléctricas del Cauca CEDELCA S.A. E.S.P.

> **SEGUNDO:** Adoptar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de CENTRALES ELECTRICAS DEL CAUCA S.A E.S.P., mediante la planeación de actividades para la mejora continua del Sistema de Gestión de Seguridad de la Información – SGSI, documento que hace parte integral de la presenta directiva.
>
> **4. RESPONSABLE**
>
> La Oficina de Informática y Telecomunicaciones es la dependencia encargada de la estructuración e implementación del plan de gestión de riesgos de la información.

Incumplimiento en lo establecido en el Manual del Sistema de Control interno vigente a la fecha, el cual contiene un módulo para la administración del riesgo, así:

	MANUAL DEL SISTEMA DE CONTROL INTERNO	Versión: 003
		Fecha de Aprobación 04-junio -2013

MODULO IV.

4. POLÍTICAS DE ADMINISTRACIÓN DE RIESGO

Modulo IV **4. Políticas de Administración de Riesgo**	4.1 Mapa de Riesgo 4.2 Política de Administración del Riesgo

Incumplimiento en lo establecido en el **decreto 1510 de 2021**, Por el cual se adicionan los capítulos 3, 4, 5, 6 Y 7 al Título 3 de la Parte 5 del Libro 2 del Decreto 1068 de 2015 Único Reglamentario del Sector Hacienda y Crédito Público, el cual dispone lo siguiente:

> "***Artículo 2.5.3.4.7. Gestión de riesgos.*** *Los códigos de propiedad contendrán lineamientos para los Gestores de Propiedad que tengan la calidad de administradores en Empresas Receptoras, dirigidos a que estos procuren que dichas empresas*

	anticipen y gestionen los riesgos empresariales que puedan afectarlas, con el propósito de salvaguardar el patrimonio público invertido en las Empresas Receptoras, y de velar por que estas generen valor económico y social. *Los Gestores de Propiedad propenderán porque las respectivas Empresas Receptoras tengan en cuenta, por lo menos, el riesgo crediticio, el riesgo de mercado, el riesgo de lavado de activos y riesgo financiación del terrorismo, el riesgo operacional, el riesgo reputacional, el riesgo de corrupción y el riesgo ambiental.* *Los Gestores de Propiedad propenderán por que la gestión integral del riesgo de las Empresas Receptoras incluya el análisis de las contingencias y circunstancias a las que estas pueden verse enfrentadas y porque establezcan mecanismos de mitigación y adaptación específicos para cada riesgo identificado."* *"**Artículo 2.5.3.5.5. Código de Gobierno Corporativo**. Los Gestores de Propiedad adelantarán acciones dirigidas a que las Empresas Receptoras adopten un Código de Gobierno Corporativo, aprobado por la Asamblea General de Accionistas, que contenga por lo menos lo siguiente:* *c. Gestión de riesgos"* *"**Artículo 2.5.3.4.4. Contenido mínimo de los códigos de propiedad**. Los códigos de propiedad deberán contener por lo menos las siguientes secciones:* 3. *Gestión de riesgos"*

8. RECURRENCIA DE HALLAZGOS DETECTADOS EN AUDITORIAS PREVIAS

AUDITORIA INTERNA VIGENCIA 2022:

Como resultado del ejercicio de auditoría interna vigencia 2022 se tienen los siguientes hallazgos:

*"**HALLAZGO ADMINISTRATIVO No.1:** No se evidencia que CEDELCA S.A. E.S.P. cuente con un esquema de publicación adoptado y difundido empresarialmente para la vigencia 2022, que permita comunicar de manera ordena, oportuna y clara la información de dominio público generada por cada uno de los procesos bajo los cuales opera su gestión, la cual debe ser divulgada a las partes interesadas y ciudadanía en general como sujeto obligado, conforme al principio de transparencia y divulgación proactiva previsto en el artículo 3 de la Ley 1712 de 2014, generando incumplimiento del artículo 12 de la misma ley el cual prevé este esquema como un requisito para los sujetos obligados."*

" ***HALLAZGO ADMINISTRATIVO No.2:*** *No se evidencia que CEDELCA S.A. E.S.P. cuente con un Registro de Activos de Información adoptado y difundido empresarialmente para la vigencia 2022, que cumpla con los estándares establecidos por el Ministerio Público y con aquellos dictados por el Archivo General de la Nación, permitiendo identificar la información producida, publicada y preservar la memoria histórica, así como facilitar la continuidad en los procesos administrativos y de gestión, generando incumplimiento del artículo 13 de la Ley 1712 de 2014 el cual prevé este registro como un requisito para los sujetos obligados."*

HALLAZGO ADMINISTRATIVO No.3: *No se evidencia que CEDELCA S.A. E.S.P. cuente con un Índice de Información Clasificada y reservada adoptado y difundido empresarialmente para la vigencia 2022, permitiendo identificar la información producida por cada proceso bajo el cual se opera la gestión, que incluya sus denominaciones, la motivación y la individualización del acto en que conste tal calificación de clasificación o reserva, de acuerdo a la constitución o la ley, generando incumplimiento del artículo 20 de la Ley 1712 de 2014 el cual prevé este índice como un requisito para los sujetos obligados".*

HALLAZGO ADMINISTRATIVO No.4: *No se evidencia la publicación de datos abiertos durante la vigencia 2022 en la página web de CEDELCA S.A. E.S.P, desconociendo la obligación de publicación de la Información mínima obligatoria respecto a servicios, procedimientos y funcionamiento y generando incumplimiento del artículo 11 de la Ley 1712 de 2014 el cual prevé estas publicaciones como un requisito para los sujetos obligados.*

HALLAZGO ADMINISTRATIVO No.5: *No se evidencia que CEDELCA S.A E.S.P. en el transcurso de la vigencia 2022 haya implementado las directrices de accesibilidad web, estándares de publicación y divulgación de contenidos e información, condiciones mínimas técnicas y de seguridad digital, condiciones mínimas de publicación de datos abiertos en cumplimiento de la Resolución N° 001519 de 24 de agosto de 2020 y sus anexos, del Ministerio de Tecnologías de la Información y las Comunicaciones como sujeto obligado en referencia al artículo 5 de la Ley 1712 del 2014, corregido por el artículo 1 del Decreto 1494 del 2015."*

En este sentido no se evidencia la recurrencia de hallazgos en el presente informe de Auditoría Interna.

AUDITORIAS EXTERNAS:

No se evidencian hallazgos recurrentes detectados inicialmente en la Auditoría Externa – CGR - vigencia 2021 realizada a CEDELCA S.A. E.S.P. en la vigencia 2022, relacionados con el proceso de Informática y Comunicaciones. En este mismo sentido no se evidencian hallazgos recurrentes detectados inicialmente en la Auditoría Externa – CGR - vigencia 2022 realizada a CEDELCA S.A. E.S.P. en la vigencia 2023, relacionados con el proceso de Informática y Comunicaciones.

9. MATRIZ DE CONTRADICCION: El auditado no presenta contradicción en relación con el Informe Preliminar.

Para constancia se firma el respectivo Informe Final de Auditoría Interna al Proceso Gestión Financiera y Administrativa - Subproceso Informática y comunicaciones el día 29 de mayo de 2023.

APROBACIÓN DEL INFORME FINAL DE AUDITORÍA INTERNA

Nombre Completo	Responsabilidad	Firma
Olga Lorena Díaz Chagüendo	Jefe de Oficina de Control Interno y de Gestión - Auditor Líder	
Luz Enith Fernández Gómez	Profesional Universitario II - Oficina de Control Interno y de Gestión - Auditor de apoyo	
Boomer Calvache Riascos	Contratista de Apoyo Oficina de Control Interno y de Gestión	