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

DIRECTIVA GERENCIAL No. 009 DE 2022

PARA: DIRECTIVOS, ASESORES Y TRABAJADORES DE LA EMPRESA

DE: GERENCIA DE CEDELCA S.A E.S.P.

ASUNTO: "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."

FECHA: 21 de septiembre 2022

El Gerente Suplente de Centrales Eléctricas del Cauca CEDELCA S.A. E.S.P., en uso de sus facultades legales y estatutarias, en especial las conferidas por el articulo 51 numeral 23 de los Estatutos vigentes de la Empresa a través de la presente Directiva Gerencial y considerando que

El Decreto 1008 de 2018, capitulo 1, política de gobierno digital, sección 1, objeto, alcance, ámbito de aplicación y principios, Artículo 2.2.9.1.1.1. *dispone que. "El presente capítulo establece lineamientos generales de la Política de Gobierno Digital para Colombia, antes estrategia de Gobierno en Línea, la cual desde ahora debe ser entendida como: el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital".*

Además, CEDELCA S.A E.S.P. debe atender los principios reglamentados en el decreto 1008 de 2018 que rezan:

"Artículo 2.2.9.1.1.3. Principios. La Política de Gobierno Digital se desarrollará conforme a los principios que rigen la función y los procedimientos administrativos consagrados en los artículos 209 de la Constitución Política, 3° de la Ley 489 de 1998, 3° de la Ley 1437 de 2011, 2° y 3° de la Ley 1712 de 2014, así como los que orientan el sector TIC establecidos en el artículo 2° de la Ley 1341 de 2009, y en particular los siguientes:

***Innovación**: En virtud de este principio el Estado y los ciudadanos deben propender por la generación de valor público a través de la introducción*

de soluciones novedosas que hagan uso de TIC, para resolver problemáticas o necesidades identificadas.

***Competitividad**: Según este principio el Estado y los ciudadanos deben contar con capacidades y cualidades idóneas para actuar de manera ágil y coordinada, optimizar la gestión pública y permitir la comunicación permanente a través del uso y aprovechamiento de las TIC.*

***Proactividad**: Con este principio se busca que el Estado y los ciudadanos trabajen de manera conjunta en el diseño de políticas, normas, proyectos y servicios, para tomar decisiones informadas que se anticipen a los acontecimientos, mitiguen riesgos y atiendan a las necesidades específicas de los usuarios, buscando el restablecimiento de los lazos de confianza a través del uso y aprovechamiento de las TIC.*

***Seguridad de la Información:** Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano"*

La Estrategia Anti-trámite y Atención Efectiva al Ciudadano y la de Gobierno Digital, buscan un mismo fin, el primero desde la racionalización del procedimiento y el segundo desde la automatización del mismo, siendo pertinente optimizar recursos y generar unidad de criterios.

Así mismo la planeación estratégica de tecnologías de la información PETI, tienen como objetivo asegurar que las metas y objetivos de Tecnologías de Información estén vinculados y alineados con las metas y objetivos de CEDELCA S.A E.S.P.

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de CEDELCA S.A E.S.P, con respecto a la protección de los activos de información(servidores públicos, contratistas, terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la entidad y apoyan la implementación del Modelo de Seguridad y Privacidad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

En ese sentido, se hace necesario que CEDELCA S.A. E.S.P. defina los criterios para la identificación, análisis, valoración, acciones y seguimientos a los

riesgos potenciales que afecten la confiabilidad, disponibilidad e integridad de la información, que le permita minimizar pérdidas y maximizar oportunidades en el manejo de la información.

Por lo tanto, se considera pertinente definir acciones y estratégicas, para fortalecer la 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.

En virtud de lo anterior se considera:

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.

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.

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

CUARTO: Divulgación: La presente Directiva del Plan Estratégico de la Información y las Comunicaciones PETI, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, Plan Estratégico de Seguridad de la información y Ciberseguridad de Centrales Eléctricas del Cauca CEDELCA S.A. E.S.P., será publicado en la página web de la empresa www.cedelca.com.co, socializaciones en el proceso de inducción y reinducción y herramienta de divulgación interna a todos los que en ella laboran, dichos planes estarán vigentes durante el periodo 2022 - 2025, alineados con el Plan Estratégico empresarial, permitiendo revisiones periódicas y modificaciones siempre que sean necesario alinear o ajustar sus metas de acuerdo con las directrices del Gobierno Nacional y de CEDELCA S.A E.S.P..

SEPTIMO: La presente Directiva rige a partir de la fecha de su expedición y deroga todas las disposiciones contrarias, en específico la contenida en la resolución 09 de enero 27 de 2021.

COMUNIQUESE Y CUMPLASE

Dada en el municipio de Popayán – Cauca a los 21 días del mes de Septiembre del año 2022

MARIA BRAVO CUELLAR
Gerente Suplente
CEDELCA S.A. E.S.P.

Elaboró: Dania Isabel Ahumada Pardo
Revisó: Fernando Andres Estrada Romero

Plan Estratégico de Seguridad de la Información y Ciberseguridad.

Mayo de 2022

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

SAB
CONSULTING SERVICES

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Establecer como habilitador transversal la seguridad y privacidad de la información, mediante la definición detallada de la implementación de controles de seguridad físicos y lógicos con el fin de asegurar de manera eficiente los trámites, servicios, sistemas de información, plataforma tecnológica e infraestructura física y del entorno de la entidad gestionando de manera eficaz, eficiente y efectiva los activos de información, infraestructura critica, los riesgos e incidentes de seguridad y privacidad de la información y así evitar la interrupción en la prestación de los servicios de negocio.

Teniendo en cuenta lo anterior, la Oficina de Informática y Telecomunicaciones define los lineamientos para la implementación de la estrategia de seguridad de la información a través de un Modelo de Seguridad y Privacidad de la Información (en adelante MSPI), con el objetivo de formalizar al interior de Cedelca un sistema de gestión de seguridad de la información – SGSI y seguridad digital, el cual contempla su operación basada en un ciclo PHVA (Planear, Hacer, Verificar y Actuar), así como los requerimientos legales, técnicos, normativos, reglamentarios y de funcionamiento.

Cedelca asume compromisos en relación con la Seguridad y Privacidad de la información y diseñará el Plan Estratégico de Seguridad y Privacidad de la Información, trazando la ruta para alcanzar en la vigencia 2022-2025 la situación objetivo que le permita tener un adecuado nivel de madurez en seguridad de la información y a partir de este estado poder garantizar la sostenibilidad aplicando el ciclo PHVA de manera constante, con el fin de apoyar el cumplimiento de los objetivos estratégicos de la entidad.

2. OBJETIVO

Definir las actividades necesarias para implementar y apropiar el Modelo de Seguridad y Privacidad de la Información para brindar confianza a los grupos de valor en cuanto al tratamiento de la información basado en la gestión de riesgos de seguridad y privacidad con el fin de proteger, preservar y administrar la confidencialidad, integridad, disponibilidad de la información.

3. ALCANCE

El Plan Estratégico de Seguridad y Privacidad de la Información (PESI) describe el estado del arte frente al componente de Seguridad de la Información enmarcados en el Sistema de Gestión de Seguridad de la Información (SGSI), así como la situación objetivo que debe alcanzar la entidad durante el periodo 2022 - 2025, con el fin de apoyar el cumplimiento de los objetivos estratégicos.

De igual forma, se traza la ruta para continuar con la implementación de la política de Seguridad Digital y lograr el estado de madurez de seguridad con el fin de proteger, preservar y administrar la confidencialidad, integridad, disponibilidad de la información.

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.

La Oficina de Informática y Telecomunicaciones es la dependencia responsable de la formulación, estructuración y seguimiento del Modelo de Seguridad y Privacidad de la Información.

Todos los empleados, contratistas y terceros con acceso a la información de la entidad son responsables de la implementación del Modelo de Seguridad y Privacidad de la Información.

5. MARCO NORMATIVO

Marco Normativo	Descripción
Ley estatutaria 1581 de 2012,	Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley 1266 de 2008	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales.
Ley 603 de 2000	El informe de gestión deberá contener una exposición fiel sobre la evolución de los negocios y la situación económica, administrativa y jurídica de la sociedad. El informe debe incluir el estado de cumplimiento de las normas sobre **propiedad intelectual y derechos de autor** por parte de la sociedad.

6. DEFINICIONES

- **Activo**: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).
- **Amenazas**: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- **Análisis de Riesgo**: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- **Auditoría**: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).
- **Autorización**: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)
- **Bases de Datos Personales**: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)
- **Ciberseguridad**: Capacidad de las entidades para minimizar el nivel de riesgo al que están expuestos los asociados, ante amenazas o incidentes de naturaleza cibernética.
- **Ciberespacio**: Ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios.
- **Control**: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Un control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el nivel de riesgo.

- **Datos Personales**: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- **Datos Personales Públicos**: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.
- **Datos Personales Sensibles**: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos.
- **Datos Personales Privados**: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)
- **Declaración de aplicabilidad**: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).
- **Derecho a la Intimidad**: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).
- **Encargado del Tratamiento de Datos**: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3)
- **Gestión de incidentes de seguridad de la información**: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
- **Ley de Habeas Data**: Se refiere a la Ley Estatutaria 1266 de 2008.
- **Ley de Transparencia y Acceso a la Información Pública**: Se refiere a la Ley Estatutaria 1712 de 2014.
- **Mecanismos de protección de datos personales**: Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.
- **Plan de continuidad del negocio**: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
- **Plan de tratamiento de riesgos**: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- **Privacidad**: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad.

- **Registro Nacional de Bases de Datos**: Directorio público de las bases de datos que contienen datos personales sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)
- **Riesgo**: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Seguridad de la información**: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- **Sistema de Gestión de Seguridad de la Información SGSI**: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).
- **Titulares de la información**: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)
- **Tratamiento de Datos Personales**: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).
- **Trazabilidad**: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).
- **Vulnerabilidad**: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).
- **Partes interesadas**: (Stakeholder) Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

7. NIVELES DE MADUREZ DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

De acuerdo con la metodología planteada en el modelo de seguridad y privacidad de la información, para lograr el nivel de madurez 5 se requiere cumplir con un número de requisitos específicos los cuales están asociados a cada nivel de madurez y están alineados al ciclo PHVA, es por esta razón que el plan de acción se encuentra estructurado por niveles de madurez y las actividades asociadas a cada nivel corresponden a los entregables o productos que se deben tener en cada uno para avanzar en la implementación del habilitador transversal "Seguridad de la Información".

A continuación, se describen de manera condensada los requisitos para cada nivel de madurez.

0. **Inexistente**
   - Se han implementado controles en su infraestructura de TI, seguridad física, seguridad de recursos humanos entre otros, sin embargo, no están alineados a un Modelo de Seguridad.
   - No se reconoce la información como un activo importante para su misión y objetivos estratégicos.
   - No se tiene conciencia de la importancia de la seguridad de la información.

1. **Inicial**

- Se han identificado las debilidades en la seguridad de la información.
- Los incidentes de seguridad de la información se tratan de forma reactiva.
- Se tiene la necesidad de implementar el MSPI, para definir políticas, procesos y procedimientos que den respuesta proactiva a las amenazas sobre seguridad de la información.

2. **Repetible**
   - Se identifican en forma general los activos de información.
   - Se clasifican los activos de información.
   - Los empleados de la entidad tienen conciencia sobre la seguridad de la información.
   - Los temas de seguridad y privacidad de la información se tratan en un comité especifico de seguridad de la información.

3. **Definido**
   - La entidad ha realizado un diagnóstico que le permite establecer el estado actual de la seguridad de la información.
   - La entidad ha determinado los objetivos, alcance y límites de la seguridad de la información.
   - La entidad ha establecido formalmente políticas de Seguridad de la información y éstas han sido divulgadas.
   - La entidad tiene procedimientos formales de seguridad de la Información.
   - La entidad tiene roles y responsabilidades asignados en seguridad y privacidad de la información.
   - La entidad ha realizado un inventario de activos de información aplicando una metodología.
   - La entidad trata riesgos de seguridad de la información a través de una metodología.
   - Se implementa el plan de tratamiento de riesgos.
   - Se revisa y monitorea periódicamente los activos de información de la entidad.
   - Se utilizan indicadores para establecer el cumplimiento de las políticas de seguridad y privacidad de la información.
   - Se evalúa la efectividad de los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro.

4. **Administrado**
   - Revisa y monitorea periódicamente los activos de información.
   - Utilizan indicadores para establecer el cumplimiento de las políticas de seguridad y privacidad de la información.
   - Evalúa la efectividad de los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro.

5. **Optimizado**
   - En este nivel se encuentran las empresas en las cuales la seguridad es un valor agregado para la organización.
   - Utilizan indicadores de efectividad para establecer si la entidad encuentra retorno a la inversión bajo la premisa de mejora en el cumplimiento de los objetivos misionales.

- Se establecen planes de mejora continua sobre las métricas y los hallazgos de auditorías internas y externas.

8. SITUACIÓN ACTUAL SEGURIDAD DE LA INFORMACIÓN

Por situación actual se entiende el nivel de madurez que posee en este momento **Cedelca** con relación a la seguridad de la información, para lo cual se recolectó información mediante el diligenciamiento de las herramientas de diagnóstico tipo GAP análisis del Sistema de Gestión de Seguridad de la Información y Ciberseguridad, la cual se documentó utilizando para la ejecución de la evaluación las siguientes fases:

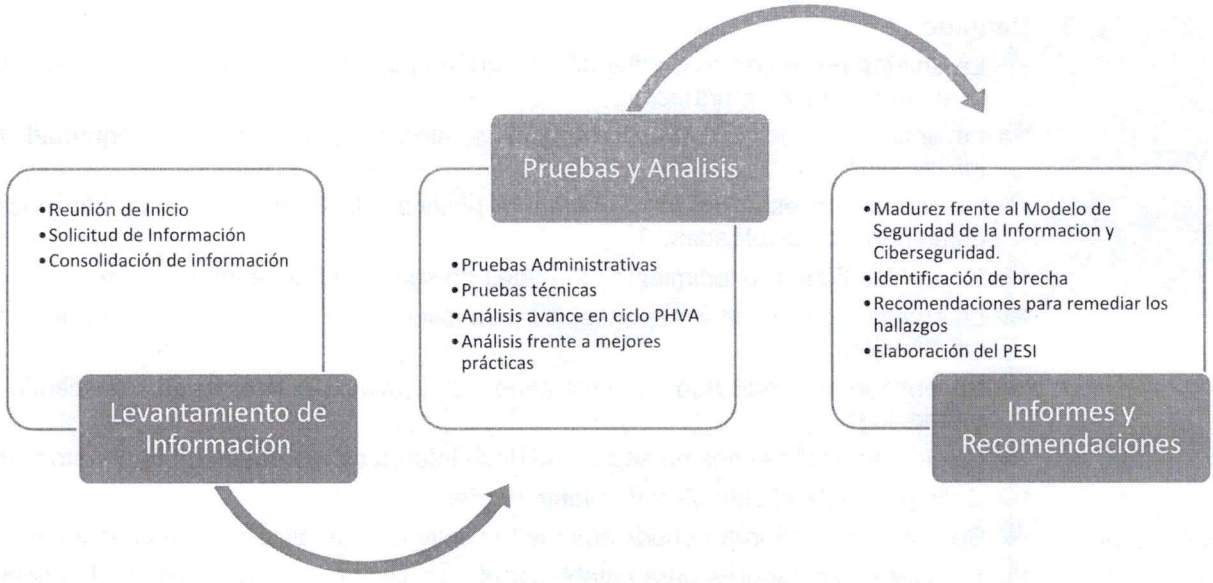


Figura 1. Fases de ejecución evaluación SGSI-CS

8.1 EVALUACIÓN DE EFECTIVIDAD DE CONTROLES

El diligenciamiento de la herramienta permitió obtener una calificación calculada para cada dominio y está totalizada a partir del valor registrado y promediado sobre la cantidad de objetivos de control que se establecen. El resultado obtenido para la evaluación del estado actual nos refleja los controles y su efectividad según la Normatividad ISO 27001 del 2013 y lo planteado dentro de las herramientas de gestión de riesgos digitales.

Con el diligenciamiento de las herramientas, se obtuvieron los siguientes resultados de los dominios para la evaluación de efectividad de los controles:

No.	Evaluación de Efectividad de controles

	DOMINIO	Calificación Actual	Calificación Planteada	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	20	100	INICIAL
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	20	95	INICIAL
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	30	85	REPETIBLE
A.8	GESTIÓN DE ACTIVOS	22	15	REPETIBLE
A.9	CONTROL DE ACCESO	54	95	EFECTIVO
A.10	CRIPTOGRAFÍA	20	60	INICIAL
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	62	95	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	52	85	EFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	53	98	EFECTIVO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	46	90	EFECTIVO
A.15	RELACIONES CON LOS PROVEEDORES	20	100	INICIAL
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	23	100	REPETIBLE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	20	75	INICIAL
A.18	CUMPLIMIENTO	27,5	90	REPETIBLE
PROMEDIO EVALUACIÓN DE CONTROLES		**34**	**84,5**	**REPETIBLE**

Tabla 1. Evaluación de efectividad de Controles - ISO 27001:2013

De acuerdo con el análisis y los resultados obtenidos, la calificación promediada de los controles dentro de la entidad fue de **34**, lo cual evidencia que **Cedelca** se encuentra en un proceso "inicial" de implementación de medidas para la seguridad y privacidad de la información, evidenciando oportunidades de mejora que se encuentra en proceso de revisión y mejora de los controles existentes.

Sin embargo, se precisan los dominios que deben ser incluidos entre las acciones de la actual vigencia para su fortalecimiento, en especial los que quedaron evaluados en estado inicial.

En estos dominios se evidencia que la calificación obtenida está por debajo del promedio total de la evaluación de controles objetivo, por lo que se tendrá en cuenta los niveles de madurez alcanzados por cada uno de los dominios, con el fin de plantear las acciones y actividades prioritarias en el plan de seguridad de la información que permita de manera rápida y significativa mejorar el nivel de madurez de la entidad.

8.2 BRECHA ANEXO A ISO 27001:2013

En este componente se muestra de manera gráfica el resultado del análisis de brecha frente a los controles del Anexo A, del estándar ISO 27001:2013. Aquí se puede evidenciar la calificación de cada dominio frente a la escala de evaluación definida y también en comparación con la calificación objetivo.

Figura 3. Fases de ejecución evaluación MPSI

De acuerdo con la evaluación realizada y los resultados obtenidos, **Cedelca** se encuentra en un proceso "Inicial" con respecto a la implementación de medidas y controles destinados a garantizar la seguridad de la información, así mismo, como la protección de los activos que la contienen.

8.3 AVANCE DEL CICLO PHVA (PLANEAR-HACER-VERIFICAR-ACTUAR)

El aspecto que determina la evaluación del estado actual en la entidad es el correspondiente al ciclo del modelo de operación PHVA. A continuación, se presenta el resultado del avance del ciclo de funcionamiento del Modelo de Operación (PHVA).

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual	% Avance Esperado

2020	Planificación	4%	40%
	Implementación	2%	20%
	Evaluación de desempeño	0%	20%
	Mejora continua	0%	20%
TOTAL		**5%**	**100%**

Tabla 2. Avance del Ciclo PHVA

El resultado presenta un porcentaje de avance del 5% a corte 4 de febrero de 2022. Según el análisis realizado, se encuentra en un proceso "inicial" de cumplimiento con respecto al PHVA y lo referente a la implementación de la ISO 27001:2013.

Para el ítem de planificación la entidad se encuentra en un 4% del 40% que debería presentar, para el ítem de Implementación la entidad se encuentra en un 2% de un total de un 20%, para el ítem de evaluación de desempeño la entidad se encuentra cumpliendo actualmente con un 0% de un total del 20% que debería presentar y para el ítem de mejora continua la entidad ha completado un 0% de un total del 20%.

Lo anterior se puede visualizar de manera precisa en la siguiente grafica de Avance Ciclo de Funcionamiento del Modelo de Operación la cual representa el avance actual en la entidad y lo esperado, mostrando las diferencias de cada fase del ciclo PHVA.

La gráfica presenta una comparación entre el avance logrado por la entidad, el avance objetivo y el avance total posible.

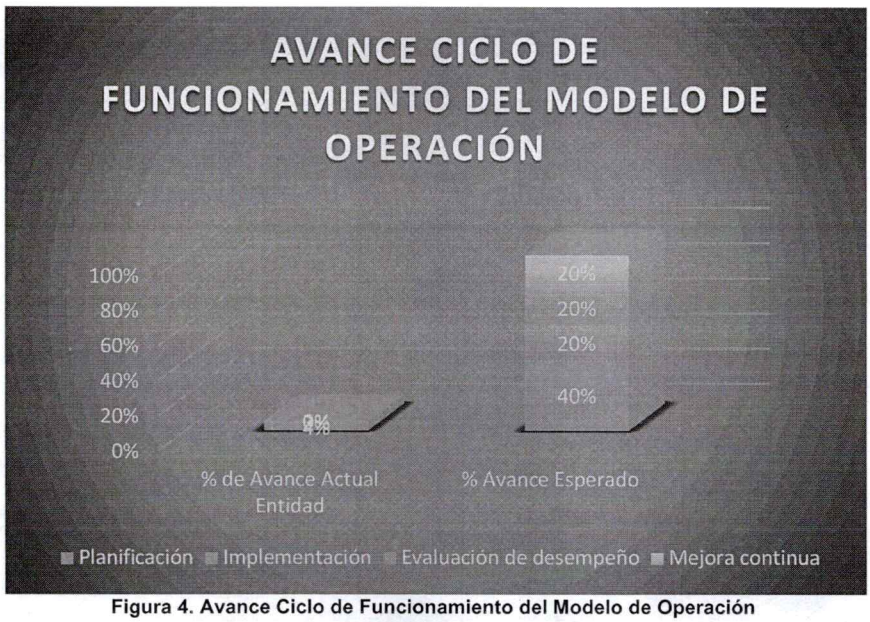


Figura 4. Avance Ciclo de Funcionamiento del Modelo de Operación

8.4 NIVEL DE MADUREZ

La madurez de la seguridad se puede medir únicamente a través de la capacidad en que la entidad utiliza de forma eficaz y eficiente los recursos disponibles para el apoyo de las funciones de forma que se cree un nivel de seguridad sostenible. Para ello debe establecerse una línea de partida de la madurez de la seguridad y usarse para definir los procesos en las que centra las actividades de seguridad de la información.

En el resultado obtenido al diligenciar las herramientas, se evidencia que la entidad se encuentra en un nivel "Inicial" de madurez y de cumplimiento de acuerdo con la implementación del Modelo de Seguridad y Privacidad de la Información. Para el Nivel 1, se ha identificado:

- Debilidades en la seguridad de la información.
- Los incidentes de seguridad de la información se tratan de forma reactiva.
- Se tiene la necesidad de implementar el MSPI, para definir políticas, procesos y procedimientos que den respuesta proactiva a las amenazas sobre seguridad de la información que se presentan en la Entidad.

Para alcanzar el nivel de optimizado se debe diseñar un plan de trabajo con las brechas identificadas y así actualizar, diseñar y revisar los controles que actualmente se encuentran en operación para la vigencia 2022 – 2025.

NIVEL DE MADUREZ MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	NIVEL DE CUMPLIMIENTO
Inicial	INTERMEDIO
Repetible	CRÍTICO
Definido	CRÍTICO
Administrado	CRÍTICO
Optimizado	CRÍTICO

Nivel	Descripción
Inicial	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información
Repetible	En este nivel se encuentran las entidades, en las cuales existen procesos procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentra gestionados dentro del componente planificación del MSPI.
Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Administrado	En este nivel se encuentran las entidades, que cuenten con métricas, indicadores y realizan auditorías al MSPI, recolectando información para establecer la efectividad de los controles.
Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.

Figura 5. Estado actual y proyección del nivel de madurez

9. PLAN DE SEGURÍDAD Y PRIVACIDAD DE LA INFORMACIÓN

Se presentan las características de cada uno de los niveles de madurez del Modelo de Seguridad y Privacidad de la Información, se presenta la fecha estimada y la correspondiente vigencia en la que se adelantarán las actividades asociadas a cada nivel de madurez.

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.

	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	**OPERACIÓN 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

El plan de trabajo será revisado de manera anual y las iniciativas estarán alineadas con el plan estratégico de la entidad y de acuerdo con los cambios y prioridades del negocio permitiendo mejorar el nivel de madurez del sistema de gestión de seguridad de la información.

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

			gestión de riesgos digitales.
5	**IMPLEMENTACION CONTROLES DEL SGSI**		
5.1	Establecer un Servicio o mecanismo de análisis de comportamiento de red (Network Behavior analytics), que permitan definir y monitorear líneas base de comportamiento de red, obteniendo así el monitoreo sobre anomalías y comportamiento fuera de esta línea base en la red, tales como altos consumos, mayores aplicaciones usadas, posible comportamiento que definan un Indicador de compromiso (IoC) que lleve hacia un fraude o malware avanzado.	II Semestre 2024	Armar el caso de negocio para tercerizar el servicio de SOC / SIEM. Implementar o contratar servicio de Centro de operaciones de seguridad (SOC) que permita identificar de manera temprana y contener los ciberataques, mediante la realización de monitoreo inteligente y la correlación de eventos e integración de fuentes (aplicaciones, App, seguridad, entre otros) para plataformas On premises y Nube. Brindando cobertura a los sistemas más críticos.
5.2	Realizar el proyecto de endurecimiento de infraestructura: servidores, bases de datos, aplicaciones, elementos activos de red	I Trimestre 2024	Llevar a cabo el ejercicio de análisis de vulnerabilidades y red team con frecuencia, mínimo una vez al mes. Establecer e implementar pruebas de Hacking Ético de manera periódica sobre los aplicativos críticos expuestos en el ciberespacio.
5.3	Diseñar estrategias del Plan de Recuperación de Desastres Tecnológico.	II Trimestre 2023	Informes de Estratégias a implementar.
5.4	Documentar planes de acción ante diferentes ciberataques, donde se especifiquen qué acciones de contención se deben adoptar (Ej. desconexión automática de equipos, cambios de contraseñas, actualizar la base de firmas del antivirus, bloqueo de direcciones IP, entre otros). Fase I.	II Trimestre 2024	Playbook de diferentes escenarios de ciberataques.
5.5	Diseñar Plan de Continuidad de Negocio. Fase I.	III Trimestre 2024	Plan de Continuidad de Negocio.
5.6	Implementar y monitorear una solución de WAF para las aplicaciones expuestas en el ciberespacio.	II Trimestre 2024	Aseguramiento de aplicativos WEB.
5.7	Análisis de vulnerabilidades en código fuente	III Trimestre 2024	Informes de resultados.
5.8	Ejecutar el programa de ejercicios al plan de recuperación ante desastres, para los escenarios de ataques cibernéticos.	III Trimestre 2024	Informes de resultados de pruebas realizadas.
5.9	Elaborar el programa de auditoría técnica anual a los terceros críticos para verificar el cumplimiento de las medidas y obligaciones establecidas en los	III Trimestre 2024	Informes de auditorias a terceros.

	contratos con el fin de verificar la adecuada gestión de los riesgos de seguridad de la información y ciberseguridad. Fase I		
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.
	Implementar Estrategias del Plan de Recuperación de Desastres Tecnológico. Fase I	III Trimestre 2024	Plan de Recuperación de Desastres - DRP
6	**PLAN DE SENSIBILIZACIÓN SEGURIDAD DE LA INFORMACIÓN**		
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.
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.
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.

No.	Actividad	Fecha fin Estimada	Producto o entregable
1	**PLANEACIÓN SGSI**		
1.1	Se establecerán las políticas y los procedimientos adicionales y se implementarán las medidas técnicas de apoyo a los procesos de negocio que permitan un gobierno de TI adecuado 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, la mano de obra y/o a los ciudadanos, basados en normas aceptadas por la industria (como ITIL y COBIT)	I Trimestre 2025	Uso y apropiación de las políticas y procedimientos de seguridad y privacidad de la información.
1.2	Actualización de riesgos digitales en todos los procesos	I Trimestre 2025	Matriz de riesgos digitales de todos los procesos de Cedelca.
2	**AUTODIAGNOSTICO MSPI**		
2.1	Realizar actualización de los niveles de madurez en los controles establecidos en las herramientas de gestión de riesgos digitales.	I Trimestre 2025	Informes de diagnóstico. Actualización SOA

3	**ACTIVOS DE INFORMACIÓN**		
3.1	Realización de campañas de clasificación de activos de información en los procesos.	II Trimestre 2025	Matrices de clasificación de activos de los procesos.
4	**IMPLEMENTACIÓN DEL SGSI**		
4.1	Diseñar e Implementar el programa anual de capacitación especializada en Ciberseguridad para los colaboradores que son responsables de Ciberseguridad.	III Trimestre 2025	Certificados de asistencia a capacitaciones en seguridad de la información y ciberseguridad.
4.2	Implementar una herramienta tipo GRC (Governance, Risk and Compliance) que permita la administración del sistema de gestión de seguridad de la información y del marco de trabajo de ciberseguridad, la administración de los activos de información, la gestión de los riesgos de ciberseguridad, la gestión de vulnerabilidades.	II Trimestre 2025	Riesgos Digitales y avances del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Continuidad de Negocio en herramienta de apoyo.
5	**OPERACIÓN DEL SGSI**		
5.1	Elaborar el programa de auditoría técnica anual a los terceros críticos para verificar el cumplimiento de las medidas y obligaciones establecidas en los contratos con el fin de verificar la adecuada gestión de los riesgos de seguridad de la información y ciberseguridad.	III Trimestre 2025	Informes de auditorias a terceros.
5.2	Implementar como servicio una solución de anti malware avanzado para la protección contra amenazas avanzadas persistentes.	I Trimestre 2025	Indicadores de amenazas materializadas.
5.4	Documentar planes de acción ante diferentes ciberataques, donde se especifiquen qué acciones de contención se deben adoptar (Ej. desconexión automática de equipos, cambios de contraseñas, actualizar la base de firmas del antivirus, bloqueo de direcciones IP, entre otros).	II Trimestre 2025	Playbook de diferentes escenarios de ciberataques.
5.5	Realizar el proyecto de endurecimiento de infraestructura: servidores, bases de datos, aplicaciones, elementos activos de red	I Trimestre 2025	Llevar a cabo el ejercicio de análisis de vulnerabilidades y red team con frecuencia, mínimo una vez al mes. Establecer e implementar pruebas de Hacking Ético de manera periódica sobre los aplicativos críticos expuestos en el ciberespacio.
5.6	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.	I Trimestre 2025	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.
5.7	Probar el Plan de Continuidad de Negocio.	II Trimestre 2025	Plan de Continuidad de Negocio.

6	PLAN DE SENSIBILIZACIÓN SEGURIDAD DE LA INFORMACIÓN		
6.1	Realización de campañas de sensibilización en seguridad y privacidad de la información	I Trimestre 2025	Encuestas y evaluaciones de las charlas de sensibilización.
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.	II Trimestre 2025	Evidencias de aplicación de recomendaciones de proveedores de seguridad informática.

No.	Actividad	Fecha fin Estimada	Producto o entregable
1	PLANEACIÓN SGSI		
1.1	Se establecerán las políticas y los procedimientos adicionales y se implementarán las medidas técnicas de apoyo a los procesos de negocio que permitan un gobierno de TI adecuado 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, la mano de obra y/o a los ciudadanos, basados en normas aceptadas por la industria (como ITIL y COBIT 5). Además, las políticas y procedimientos deberán incluir roles y responsabilidades definidos, apoyados por una formación regular de la mano de obra.	I Trimestre 2025	Uso y apropiación de las políticas y procedimientos de seguridad y privacidad de la información.
1.2	Actualización de riesgos digitales en todos los procesos	I Trimestre 2025	Matriz de riesgos digitales de todos los procesos de Cedelca.
1.3	Establecer presupuesto de Seguridad de la Información y Ciberseguridad	II Trimestre 2025	PESI cuantificado.
2	AUTODIAGNOSTICO MSPI		
2.1	Realizar actualización de los niveles de madurez en los controles establecidos en la herramienta de diagnóstico.	I Trimestre 2025	GAP análisis actualizado en herramientas de gestión de riesgos digitales.
3	ACTIVOS DE INFORMACIÓN		
3.1	Realización de campañas de clasificación de activos de información en los procesos.	II Trimestre 2025	Matrices de clasificación de activos de los procesos.
4	IMPLEMENTACIÓN DEL SGSI		
4.1	Diseñar e Implementar el programa anual de capacitación especializada en Ciberseguridad para los colaboradores que son responsables de Ciberseguridad.	II Trimestre 2025	Certificados de asistencia a capacitaciones en seguridad de la información y ciberseguridad.
5	OPERACIÓN DEL SGSI		
5.1	Elaborar el programa de auditoría técnica anual a los terceros críticos para verificar el cumplimiento de las medidas y obligaciones establecidas en los contratos con el fin de verificar la adecuada gestión	II Trimestre 2025	Informes de auditorias a terceros.

	de los riesgos de seguridad de la información y ciberseguridad.		
5.2	Documentar planes de acción ante diferentes ciberataques, donde se especifiquen que acciones de contención se deben adoptar (Ej. desconexión automática de equipos, cambios de contraseñas, actualizar la base de firmas del antivirus, bloqueo de direcciones IP, entre otros).	II Trimestre 2025	Playbook de diferentes escenarios de ciberataques.
5.3	Realizar el proyecto de endurecimiento de infraestructura: servidores, bases de datos, aplicaciones, elementos activos de red	I Trimestre 2025	Llevar a cabo el ejercicio de análisis de vulnerabilidades y red team con frecuencia, mínimo una vez al mes. Establecer e implementar pruebas de Hacking Ético de manera periódica sobre los aplicativos críticos expuestos en el ciberespacio.
5.4	Ejecutar el programa de ejercicios al plan de recuperación ante desastres, para los escenarios de ataques cibernéticos.	III Trimestre 2025	Informes de resultados de pruebas realizadas.
5.5	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.	I Trimestre 2025	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.
5.6	Probar el Plan de Continuidad de Negocio.	II Trimestre 2025	Plan de Continuidad de Negocio.
6	**PLAN DE SENSIBILIZACIÓN SEGURIDAD DE LA INFORMACIÓN**		
6.1	Realización de campañas de sensibilización en seguridad y privacidad de la información	I Trimestre 2025	Encuestas y evaluaciones de las charlas de sensibilización.
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 2025	Evidencias de aplicación de recomendaciones de proveedores de seguridad informática.

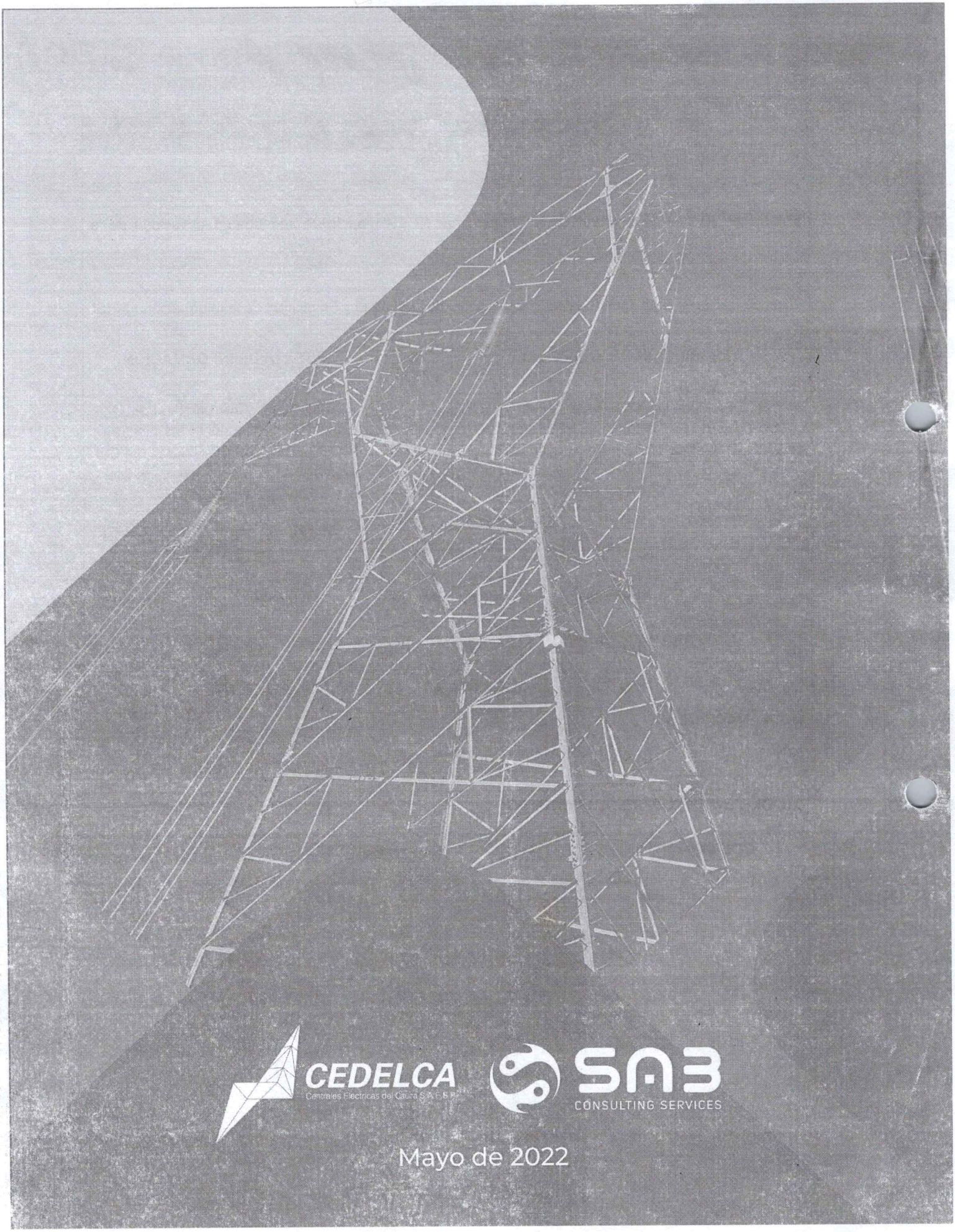
9.1 INDICADOR

MADUREZ SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	
RESPONSABLE	Oficial de Seguridad de la Información
DEFINICIÓN:	

MADUREZ SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN					
El indicador permite medir el nivel de madurez del SGSI					
OBJETIVO					
Establecer el nivel de madurez de la implementación del modelo de seguridad y privacidad de la información para establecer el estado de la gestión y adopción de controles.					
FÓRMULA					
Nivel de madurez en la implementación del Modelo de seguridad y Privacidad de la Información - MPSI					
DESCRIPCIÓN DE VARIABLES			**UNIDAD DE MEDIDA**	**FUENTE DE INFORMACIÓN**	
Resultado de la implementación frente a los controles de Seguridad de la Información y Ciberseguridad y el anexo A de la ISO 27001:2013			%	Autodiagnóstico Instrumentos de evaluación de diagnósticos de las herramientas de gestión de riesgos digitales.	
COBERTURA	**ESCALA**	**TENDENCIA**	**TIPO**	**FRECUENCIA**	
				RECOLECCIÓN	**REVISIÓN**
Modelo de Seguridad y Privacidad de la Información	Porcentaje	Decreciente	Eficacia	Semestral	Semestral
METAS					
MÍNIMA	60%	SATISFACTORIA	70%	SOBRESALIENTE	100%
OBSERVACIONES					
N/A					

10. DOCUMENTOS RELACIONADOS

CÓDIGO	DOCUMENTO


CEDELCA
Centrales Electricas del Cauca S.A.E.S.P.
SAB
CONSULTING SERVICES
Mayo de 2022