PLAN ANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION Y CIBERSEGURIDAD 2025

SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION - SGSI
SISTEMA DE ADMINISTRACION DE RIESGOS DE SEGURIDAD DE LA INFORMACION Y CIBERSEGURIDAD - SARSICIB
VICEPRESIDENCIA DE RIEGOS
FINDETER

CÓDIGO: GR-DA-035
VERSIÓN 7
CLASIFICACIÓN: Pública

Bogotá, D.C. 14 de febrero de 2025

Contenido

1. INTRODUCCIÓN

FINDETER es consciente que la protección y aseguramiento de su información es fundamental para garantizar su debida gestión financiera, administrativa y operativa, razón por la cual ha establecido un Sistema de Gestión de Seguridad de la Información - SGSI basado en la norma ISO 27001, que contempla políticas, procedimientos, límites, roles, responsabilidades y obligaciones frente a la seguridad y privacidad de la información de la entidad.

Asi mismo, FINDETER ha establecido un Sistema de Administración de Riesgos de Seguridad de la Informacion y Ciberseguridad denominado SARSICIB para la debida administración y gestión de las situacione de riesgos que atentan contra la seguridad de la información, seguridad digital y ciberseguridad de la entidad. Este sistema esta totalmente alineado con el Sistema Integral de Riesgos Operativos de FINDETER, cuyo objetivo primordial es garantizar que dichos riesgos sean conocidos, gestionados y tratados de forma documentada, sistemática, estructurada, repetible y eficiente.

A través de estos sistemas, FINDETER gestiona y administra los riesgos, eventos, amenazas, vulnerabilidades y situaciones asociadas a la seguridad de la información, la seguridad digital y la ciberseguridad, lo anterior en cumplimiento con los requerimientos del negocio y con los lineamientos, recomendaciones, requerimientos y disposiciones legales vigentes relacionas con seguridad de la información dadas por el Gobierno Nacional y la Superintendencia Financiera de Colombia – SFC, tales como:

- Circular Básica Jurídica (CE029/2014) de la Superintendencia Financiera de Colombia, así como las respectivas circulares que la adicionan, modifican o substituyan, por ejemplo: CE007/2018 que establece requerimientos mínimos para la gestión de la seguridad de la información y la ciberseguridad, CE008/2018 que establece requerimientos de seguridad y calidad en el manejo de información en la prestación de servicios financieros, CE005/2019 que establece reglas relativas al uso de servicios de computación en la nube aplicables a las entidades vigiladas y CE033/2020 que establece instrucciones relacionadas con la Taxonomía Única de Incidentes Cibernéticos – TUIC, el formato para el reporte de métricas de seguridad de la información y ciberseguridad y el protocolo de etiquetado para el intercambio de información Traffic Light Protocol (TLP).
- Política Nacional de Seguridad Digital, así como las respectivas políticas, directrices y requerimientos que al respecto surjan o que la adicionen, modifiquen o substituyan.
- Modelo de seguridad y privacidad de la información como habilitador de la política de Gobierno Digital.
- Regulación de protección de Datos personales, así como las respectivas leyes y decretos que al respecto surjan o que la adicionen, modifiquen o substituyan.

- Normatividad de transparencia y derecho de acceso a la información pública nacional, así como las respectivas leyes y decretos que al respecto surjan o que la adicionen, modifiquen o substituyan.
- Resolución 500 de 2021, Ministerio de Tecnologías de la Información y las Comunicaciones, por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
- Entre otras.

El presente documento contiene el Plan de Seguridad de la Informacion y Ciberseguridad para el año 2025, que incluye una serie de actividades para asegurar y preservar la operación, mejora continua y sostenibilidad tanto del Sistema de Gestión de Seguridad de la Información 'SGSI' como del Sistema de Administración de Riesgos de Seguridad de la Información y Ciberseguridad 'SARSICIB' de FINDETER.

En cumplimiento a lo establecido en el Decreto 612 de 2018, por medio de este documento se actualiza el Plan anual de Seguridad y Privacidad de la Información y Ciberseguridad de FINDETER.

2. OBJETIVO PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2.1. OBJETIVO GENERAL

Establecer las actividades para el establecimiento, operación, mejora continua y sostenibilidad del Sistema de Gestión de Seguridad de la Información 'SGSI' y el Sistema de Administración de Riesgos de Seguridad de la Información y Ciberseguridad 'SARSICIB' de FINDETER, acorde con los requerimientos del negocio y los lineamientos y requerimientos de seguridad de la información, seguridad digital y ciberseguridad establecidos en el Modelo de Seguridad y Privacidad como habilitador de la política de Gobierno Digital del Gobierno Nacional y en cumplimiento a las disposiciones legales vigentes emitidas por la Superintendencia Financiera de Colombia - SFC.

2.2. OBJETIVO ESPECIFICOS

Los siguientes son los objetivos específicos del Plan de Seguridad de la Información y de Ciberseguridad para el año 2025 que apalancan el cumplimiento del objetivo general y los del Sistema de Gestión de Seguridad de la Información 'SGSI' de la entidad:

OE1. Apoyar la operación, mejora continua y sostenibilidad del SGSI y SARSICIB de FINDETER. (Objetivos No. 8 y 9 SGI).

OE2. Fortalecer y optimizar la gestión de la seguridad de la información, seguridad digital y ciberseguridad al interior de FINDETER (Objetivo No. 10 SGI).

OE3. Fortalecer y optimizar la gestión de las alarmas, eventos, incidentes y vulnerabilidades que afecten la seguridad de la información y ciberseguridad de la entidad (Objetivo No. 10 SGI).

OE4. Fortalecer la gestión integral de riesgos operativos que incluye los asociados a seguridad de la información y ciberseguridad (Objetivo No. 8 SGI)

OE5. Fortalecer la cultura de seguridad de la información y ciberseguridad en FINDETER (Objetivo No. 9 SGI).

OE6. Atender las observaciones, recomendaciones hallazgos de las auditorías internas y externas de control y vigilancia (Objetivos No. 9 y 10 SGI).

OE7. Atender los requerimientos de seguridad de la información, seguridad digital y ciberseguridad establecidos por el Gobierno Nacional y la SFC (Objetivos No. 8 y 10 SGI).

OE8. Mantener la certificación de la ISO 27001 de acuerdo con el alcancel de SGSI de la entidad. (Objetivos No. 8, 9 y 10 SGI).

3. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

La Financiera de Desarrollo Territorial S.A. - FINDETER consciente de la importancia de proteger los activos de información que soportan la operación y continuidad del negocio frente a los riesgos que puedan afectar su seguridad, establece políticas, responsabilidades, procedimientos e instructivos, que representan la posición de la Junta Directiva y Equipo Directivo con respecto a la implementación, operación y sostenibilidad del Sistema de Gestión de Seguridad de la Información 'SGSI' y del Sistema de Administración de Riesgos de Seguridad de la Información y Ciberseguridad 'SARSICIB' de la entidad, en cumplimiento de la normatividad vigente. (Aprobación inicial: Junta Directa 28 de mayo de 2019, Acta No. 351).

4. ESTADO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

FINDETER cuenta con un Sistema de Gestión de Seguridad de la Información - SGSI certificado en la norma ISO 27001, cuya gestión bajo un modelo de mejora continua, nos ha permitido proteger, presentar y fortalecer la seguridad institucional para la debida gestión financiera, administrativa y operativa de la organización y nos convierte en una empresa con altos estándares de seguridad y calidad.

Así mismo, tenemos establecido un Sistema de Administración de Riesgos de Seguridad de la Información y Ciberseguridad denominado SARSICIB que hace parte de nuestro Sistema Integrado de Administración de Riegos, y cuyo objetivo primordial es asegurar que los riesgos que atentan contra la Disponibilidad, Integridad y Confidencialidad de los activos de información de FINDETER, sean conocidos, gestionados y tratados de forma oportuna, sistemática, documentada, estructurada, repetible y eficiente.

A través de estos sistemas, gestionamos y administramos las amenazas, eventos, incidentes, vulnerabilidades y aquellas situaciones de riesgos que atentan contra la seguridad de la información, la seguridad digital y la ciberseguridad de la entidad, lo anterior en atención a las necesidades y requerimientos tanto del negocio como de nuestras partes interesadas, y en cumplimiento a las disposiciones normativas, lineamientos y recomendaciones que en materia de seguridad expide la Superintendencia Financiera de Colombia – SFC y el Gobierno Nacional.

Contamos con Políticas de Seguridad de la Información y Ciberseguridad y de Administración de Riesgos aprobadas por la Junta Directiva, que establecen las medidas, limites, roles, responsabilidades y controles para la debida gestión de la seguridad de la información y la ciberseguridad de FINDETER y que son fundamentales para garantizar la operación, mejora continua, sostenibilidad y continuidad de nuestro Sistema de Gestión de Seguridad de la Información.

Considerando que el estándar normativo ISO 27001 sobre el cual la entidad se encuentra certificado surtió una actualización que implicó el cambio de su versión a la 2022, Findeter ha estructurado y desarrollado un plan de trabajo para adaptar y actualizar su Sistema de Gestión de la Seguridad de la

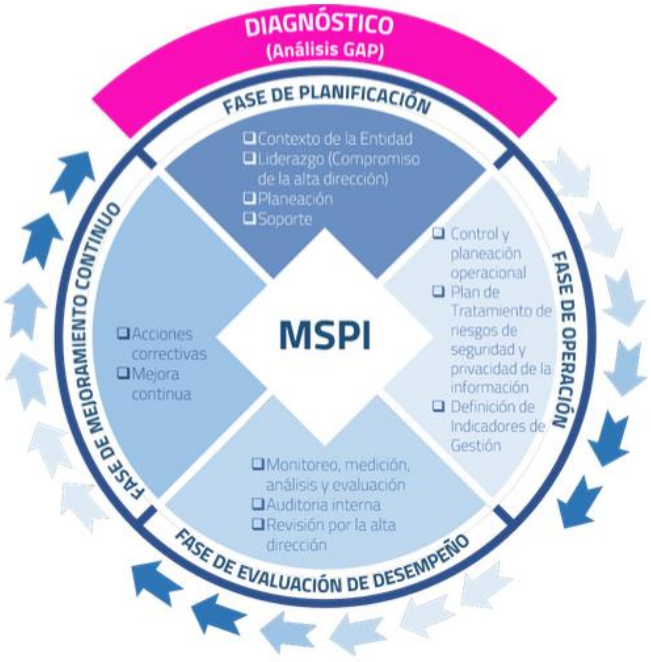
Información con el fin de cumplir los requisitos de dicha versión dentro de los plazos establecidos para su transición y lograr durante el 2025 la recertificación para los procesos que soportan el alcance del sistema y que corresponde a "Manejo de la información de las actividades relacionadas con la vinculación del cliente y la operación de los productos de Redescuento y Crédito Directo gestionados en la Sede Central.". Lo anterior, refuerza la integración de los procesos, demuestra el compromiso y la cultura de la mejora continua, fortalece la credibilidad y la imagen de la organización, y genera confianza entre nuestras partes interesadas, el Gobierno Nacional y los entes de control con relación a la aplicación de buenas prácticas en la organización en torno a la seguridad de la información y la ciberseguridad.

5. METODOLOGÍA ESTABLECIMIENTO MODELO DE SEGURIDAD

El Sistema de Gestión de Seguridad de la Información SGSI de FINDETER, se ha establecido bajo en un modelo PHVA, el cual está totalmente integrado el Sistema Integrado de Gestión de la entidad.

5.1. CICLO OPERACIÓN

El modelo de seguridad de la información de FINDETER se estableció teniendo en cuenta las cinco (5) fases definidas en el ciclo de operación del Modelo de Seguridad y Privacidad de la Información como habilitador de la política de Gobierno Digital del Gobierno Nacional [1]:



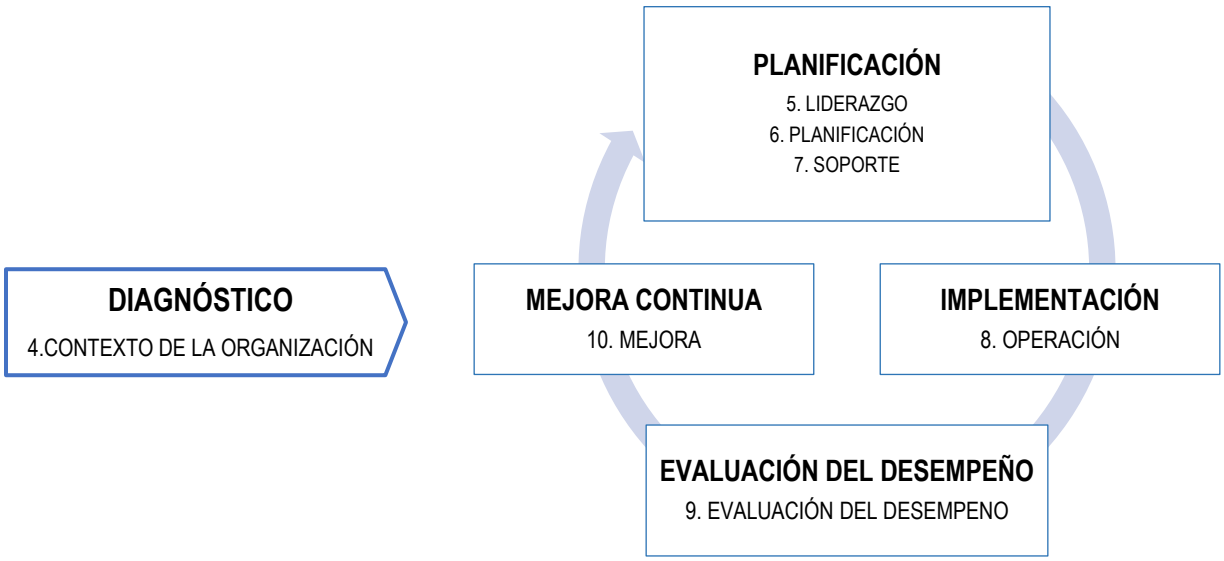
Ciclo del Modelo de Seguridad y Privacidad de la Información
Fuente: Documento Maestro del Modelo de Seguridad y Privacidad de la Información Versión 4.0 MinTIC

[1] Anexo 1 - Modelo de Seguridad y Privacidad de la Información Versión 4.0, MINTIC, febrero 2021, Pág. 6-8.

- **Fase Diagnostico**: Permite identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad de la Información.
- **Fase Planificación (P**lanear**):** En esta fase se establecen los objetivos a alcanzar y las actividades del proceso susceptibles de mejora, así como los indicadores de medición para controlar y cuantificar los objetivos.
- **Fase Implementación (H**acer**):** En esta fase se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas.
- **Fase Evaluación de desempeño (V**erificar**):** Una vez implantada la mejora, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas.
- **Fase Mejora Continua (A**ctuar**):** Se analizan los resultados de las acciones implementadas y si estas no se cumplen los objetivos definidos se analizan las causas de las desviaciones y se generan los respectivos planes de acciones.

5.2. ALINEACIÓN NORMA ISO 27001VS CICLO DE OPERACIÓN

Aunque en la norma ISO 27001 no se determina un modelo de mejora continua (PHVA) como requisito para estructurar los procesos del Sistema de Gestión de Seguridad de la Información, la nueva estructura de esta versión se puede alinear con el ciclo de mejora continua de las modelos de gestión de la siguiente forma:



Norma ISO 27001 alineado al Ciclo de mejora continua

A continuación, se muestra la relación entre las fases del ciclo de operación del Modelo de Seguridad y Privacidad de la Información (Diagnostico, Planificación, Implementación, Evaluación, Mejora Continua) y la estructura de capítulos y numerales de la norma ISO 27001:

Tabla 1. Fases Ciclo Operación vs Estructura ISO 27001

Fase	Capitulo ISO 27001:2022
Diagnostico	4. Contexto de la Organización
Planificación	5. Liderazgos 6. Planificación 7. Soporte
Implementación	8. Operación
Evaluación de desempeño	9. Evaluación de desempeño
Mejora Continua	10. Mejora

- **Fase DIAGNÓSTICO en la norma ISO 27001.** En el **capítulo 4 - Contexto de la organización** de la norma ISO 27001, se determina la necesidad de realizar un análisis de las cuestionas externas e internas de la organización y de su contexto, con el propósito de incluir las necesidades y expectativas de las partes interesas de la organización en el alcance del modelo de seguridad de la información.

- **Fase PLANEACIÓN en la norma ISO 27001.** En el **capítulo 5 - Liderazgo**, se establece las responsabilidades y compromisos de la Alta Dirección respecto al Sistema de Gestión de Seguridad de la Información y entre otros aspectos, la necesidad de que la Alta Dirección establezca una política de seguridad de la información adecuada al propósito de la organización asegure la asignación de los recursos para la seguridad de la información y que las responsabilidades y roles pertinentes a la seguridad de la información se asignen y comuniquen.
  En el **capítulo 6 - Planeación**, se establece los requerimientos para la valoración y tratamiento de riesgos de seguridad y para la definición de objetivos viables de seguridad de la información y planes específicos para su cumplimiento.
  En el **capítulo 7 - Soporte** se establece que la organización debe asegurar los recursos necesarios para el establecimiento, implementación y mejora continua del modelo de seguridad de la Información.

- **Fase IMPLEMENTACIÓN en la norma ISO 27001.** En el **capítulo 8 - Operación** de la norma ISO 27001, se indica que la organización debe planificar, implementar y controlar los procesos necesarios para cumplir los objetivos y requisitos de seguridad y llevar a cabo la valoración y tratamiento de los riesgos de la seguridad de la información.

- **Fase EVALUACIÓN DEL DESEMPEÑO en la norma ISO 27001.** En el **capítulo 9 - Evaluación del desempeño,** se define los requerimientos para evaluar periódicamente el desempeño de la seguridad de la información y eficacia del sistema de gestión de seguridad de la información.

- **Fase MEJORA CONTINUA en la norma ISO 27001.** En el **capítulo 10 - Mejora**, se establece para el proceso de mejora del modelo de seguridad de la Información, que a partir de las no-conformidades que ocurran, las organizaciones deben establecer las acciones más efectiva para solucionarlas y evaluar la necesidad de acciones para eliminar las causas de la no conformidad con el objetivo de que no se repitan.

5.3. FASE I: DIAGNÓSTICO

En el 2014, FINDETER realizó un diagnóstico en nivel de cumplimiento del Sistema de Gestión de Seguridad de la Información de acuerdo con los requerimientos establecidos en la norma ISO 27001 bajo la versión 2013, sobre la cual se base el Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno Digital.

En el mes de octubre de 2022 se publicó la nueva versión de la norma **ISO/IEC 27001:2022** que fue renombrada como "*Seguridad de la información, ciberseguridad y protección de la privacidad - Sistemas de gestión de la seguridad de la información - Requisitos*", la cual sustituye a la norma ISO 27001:2013. Esta nueva norma optimiza el uso de los controles relacionados en el Anexo A debido a que los organizó en solo cuatro secciones en comparación con las 14 de la versión 2013 y suprimió e incorporó controles para abordar las exigencias regulatorias actuales, nuevos escenarios tecnológicos, temas de ciberseguridad, servicios en la nube y privacidad de datos sobre los cuales no se había puesto el debido enfoque en la edición anterior, entendiendo que esta se produjo en el año 2013.

En agosto de 2022 el Foro Internacional de Acreditación – IAF publicó el documento mandatorio IAF MD 26:2022 "TRANSITION REQUIREMENTS FOR ISO/IEC 27001:2022", que establece un periodo de transición para esta norma de tres (3) años finalizando el 24 de octubre de 2025. También se indica, que a partir del 1 de mayo de 2024 todas las certificaciones iniciales deberán realizarse acorde a la versión 2022 y se recomienda que todas las auditorías de recertificación se hagan bajo esta nueva versión[2].

Para atender lo anteriormente expuesto, en el 2023 se realizó un nuevo diagnostico para verificar el nivel de cumplimento de la entidad con relación a los requerimientos establecidos en la versión 2022 de la norma ISO 27001 así como los cambios realizados en su anexo A. Producto de este diagnóstico, se estableció el proyecto de migración de la norma ISO 27001 de la versión 2013 a la 2022 para ser ejecutado hasta finales del año 2024.

[2] https://www.icontec.org/wp-content/uploads/2023/03/PLAN-TRANSICION-ISOIEC-27001-2013-A-VERSION-2022.pdf

En el mes de septiembre de 2024 se llevó a cabo la primera auditoría interna al SGSI sobre la norma ISO 27001:2022 durante cual no fue posible validar la implementación y operatividad de los controles dependientes del proceso de Gestión de Tecnología considerando la migración tecnológica que se encontraba en curso en ese momento. Lo anterior implicó la extensión del cierre del proyecto denominado "Transición ISO 27001 versión 2013 a versión 2022", teniendo en cuenta que fue necesario programar una auditoria complementaria en el mes de enero del año 2025 para evaluar la efectividad de los controles de seguridad implementados y mejorados durante el proceso de migración de la infraestructura tecnológica de la entidad. Con base en lo anterior, la meta del proyecto se modificó a 90% para el año 2024 reportando un avance de ejecución del plan de trabajo establecido con un cumplimiento del 85% sobre el avance proyectado y ampliando la fecha de cierre para el primer trimestre del año 2025. El control de cambios que implicó modificar la meta de esta actividad, así como los porcentajes de avance sobre su ejecución fueron informados y avalados por los líderes de los procesos involucrados.

Con relación a la fase de diagnóstico se llevó a cabo las siguientes actividades:

Metas	Actividades \ Instrumentos \ Resultados
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad	Diagnóstico de la situación actual de la entidad con relación a la gestión de seguridad de la información. Revisión por la Dirección. Valoración estado actual de la gestión de seguridad de la entidad con base en el Instrumento de Evaluación MSPI de MINTIC. Diagnostico nivel de cumplimiento de la entidad frente a los objetivos de control y controles establecidos en el Anexo A de la norma ISO 27001. Revisión de los cambios establecido entre la versión 2013 y 2022 de la norma ISO 27001 y establecimiento de los planes de acción para el cierre de las brechas encontradas.
Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad.	Valoración del nivel de estratificación de la entidad frente a la seguridad de la información con base en el método planteado en el documento '*ANEXO 3: ESTRATIFICACIÓN DE ENTIDADES*' del modelo seguridad de la información para la estrategia de Gobierno en Línea 2.0. Valoración del nivel de madurez de seguridad y privacidad de la información en la entidad de acuerdo con los lineamientos establecidos en el capítulo '*MODELO DE MADUREZ*' del documento Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno en Línea.
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Ejecución prueba de vulnerabilidades con el fin de identificar el nivel de seguridad y protección de los activos de información de la entidad y definición de planes de mitigación. Estas pruebas se realizan de forma periódica en la entidad.

5.4. FASE II: PLANIFICACIÓN

En esta fase se estableció el alcance, objetivos, procesos y procedimientos pertinentes a la gestión del riesgo y mejora de seguridad de la información, en procura de los resultados que permitan dar cumplimiento con las metas propuestas del SGSI. Para tal efecto, se han desarrollado o desarrollan las siguientes actividades dentro de un modelo de mejora continua:

Metas	Actividades \ Instrumentos \ Resultados
Realizar un análisis de Contexto y factores externos e internos de la Entidad en torno a la seguridad de la información.	El Análisis de Contexto de la entidad entorno a la seguridad de la información teniendo en cuenta el capítulo 4. CONEXTO DE LA ORGANIZACIÓN de la norma ISO 27001, con el fin de poder determinar las cuestiones externas e internas de la organización que son pertinentes para la implementación del Sistema de Gestión de Seguridad de la Información SGSI, está incluido dentro del plan estratégico de la entidad.
Definir el alcance del SGSI de la entidad	El alcance del Sistema de Gestión de Seguridad de la Información de la entidad fue aprobado por la Alta Dirección en la respectiva reunión de Revisión por la Dirección del sistema.
Definir Roles, Responsables y Funciones de seguridad y privacidad de la información	La entidad cuenta con una estructura organizacional que contempla los roles y responsabilidad pertinentes a la seguridad de la información. Las funciones de seguridad de la información están definidas tanto para el Comité de Riesgos y Comité MIPG de la entidad como para los colaboradores que ejercen los roles y responsabilidades para la implementación, administración, operación y gestión de la seguridad de la información en la entidad.
Definir la metodología de riesgos de seguridad de la información	La entidad tiene implementada una metodología integral de riegos operativos denominada SARI, que incluye los riesgos de seguridad de la información, seguridad digital, ciberseguridad y protección de datos personales.
Elaborar las políticas de seguridad y privacidad de la información de la entidad	La entidad cuenta con una Política General de Seguridad y Privacidad de la Información y unas políticas especificadas que son aprobadas por la Junta Directiva.
Elaborar documentación de operación (formatos de procesos, procedimientos y documentos debidamente definidos y establecidos) del sistema de seguridad de la información	Con relación a los documentos de operación del sistema de seguridad de la información y en cumplimiento a lo establecido en la norma ISO 27001, la entidad cuenta con la siguiente documentación controlada en el Sistema Integrado de Gestión: • Declaración de aplicabilidad • Procedimiento y/o guía de identificación y clasificación de activos de información • Procedimiento Continuidad del Negocio, Procedimientos operativos para gestión de TI • Procedimiento para control de documentos • Procedimiento para auditoría interna • Procedimiento para medidas correctivas

	• Procedimiento para la gestión de eventos e incidentes de seguridad de la información • Procedimiento para la gestión de vulnerabilidades de seguridad de la información • Gestión de la seguridad en los proveedores • Entre otros,
Identificar y valorar activos de información	La identificación y valoración de los activos de información de la entidad de acuerdo con su nivel de criticidad y el alcance del modelo de seguridad, es una labor que se realiza de forma permanente en la entidad.
Identificar, valorar y tratar los riesgos de seguridad de la información de la entidad	La identificación y valoración de los riesgos asociados a seguridad de la información, seguridad digital y ciberseguridad y la definición de los respectivos planes de tratamiento, es una actividad que se realiza de forma periódica en la entidad
Establecer plan de capacitación, comunicación y sensibilización de seguridad de la información.	En la entidad se establecen y desarrollan planes periódicos de capacitación y sensibilización en temas de seguridad de la información, ciberseguridad y riesgos.

5.5. FASE III: IMPLEMENTACIÓN

Para la implementación de la fase de planificación del SGSI, se ha tenido en cuenta los aspectos más relevantes en los procesos de implementación y/o establecimiento del Sistema de Gestión de Seguridad de la Información de la entidad. Las siguientes son actividades que se desarrollan dentro de un proceso de mejora continua:

Metas	Actividades \ Instrumentos \ Resultados
Establecer el plan de implementación de seguridad de la información	La entidad cuenta con un Sistema de Gestión de Seguridad de la Información implementado y puesto en operación, el cual se revisa anualmente y cuyos resultados se presentan en las sesiones de Revisión por la Dirección del comité de presidencia.
Ejecutar el plan de tratamiento de riesgos	La entidad tiene implementado un sistema integral de administración de riegos operativos denominada SARI, que incluye los riesgos de seguridad de la información, seguridad digital, ciberseguridad y protección de datos personales. En este sistema se establecen y se hace seguimiento a los planes de tratamiento de riegos.
Establecer indicadores de gestión de seguridad	El Sistema de Gestión de Seguridad de la Información de la entidad tiene establecidos una serie de indicadores para medir la gestión del modelo de seguridad y verificar la eficacia y efectividad de los controles implementados para mitigar los riesgos de seguridad de la entidad.
Implementar procedimiento de gestión de eventos e incidentes de seguridad	Se cuenta con los procedimientos y los mecanismos para la gestión de los eventos e incidentes de seguridad de la información y de ciberseguridad.

Implementar procedimiento de gestión de vulnerabilidades	Periódicamente en la entidad se realizan análisis de seguridad y de vulnerabilidades para determinar el nivel de protección y de seguridad de los diferentes componentes tecnológicos de la entidad.
Ejecutar plan de capacitación y sensibilización de seguridad	En la entidad se establecen y desarrollan planes periódicos de capacitación y sensibilización en temas de seguridad de la información, ciberseguridad y riesgos.
Ejecutar pruebas anuales de vulnerabilidades e intrusión	Periódicamente en la entidad se realizan análisis de seguridad y de vulnerabilidades para determinar el nivel de protección y de seguridad de los diferentes componentes tecnológicos de la entidad. Para tal efecto, se tienen en cuenta los respectivos requerimientos de seguridad relacionados con pruebas de vulnerabilidades establecidos en la circular externa 029 de 2014 de la Superfinanciera de Colombia.
Ejecutar pruebas de Ingeniera Social	Se realizan pruebas de ingeniería social de forma anual orientadas a verificar aspectos como: (i) los protocolos internos de seguridad, (ii) el nivel de concientización de los funcionarios y terceros que laboren en la entidad sobre temas de seguridad de la información, (iii) el conocimiento y/o cumplimiento de las políticas de seguridad y privacidad de la información de la entidad y (iv) el nivel de exposición de la información publicada en internet de la entidad y de sus empleados.

5.6. FASE IV: EVALUACION DE DESEMPEÑO

Periódicamente se evalúa el desempeño y la eficacia del SGSI, a través de instrumentos que permiten determinar la efectividad del sistema, tales como:

Metas	Actividades \ Instrumentos \ Resultados
Ejecución de auditorías de seguridad de la información	Se realizan auditorías del modelo de seguridad y de temas normativos y de cumplimiento de seguridad de la información aplicables a la entidad, de acuerdo con el plan de auditoria revisado y aprobado por la Alta Dirección. Las auditorías internas se llevan a cabo para revisar el modelo de seguridad de la información y ciberseguridad implementado en la entidad, con la finalidad de verificar que los objetivos de control, controles, procesos y procedimientos del modelo de seguridad cumplan con los requisitos establecidos en la norma ISO 27001
Plan de seguimiento, evaluación y análisis de SGSI	La entidad cuenta con un Sistema de Gestión de Seguridad de la Información implementado y puesto en operación, el cual se revisa anualmente y cuyos resultados se presentan en las sesiones de Revisión por la Dirección del comité de presidencia

5.7. FASE V: MEJORA CONTINUA

De acuerdo con los resultados obtenidos del componente de evaluación de desempeño se diseñan los planes de mejoramiento continuo del Sistema de Gestión de Seguridad de la Información para asegurar su debida implementación, operación y mejora continua.

Metas	Actividades \ Instrumentos \ Resultados
Diseñar plan de mejoramiento	**Se diseñan planes de mejoramiento continuo de seguridad** y privacidad de la información, que permiten realizar el plan de implementación de los hallazgos identificados para el Sistema de Gestión de Seguridad de la Información.

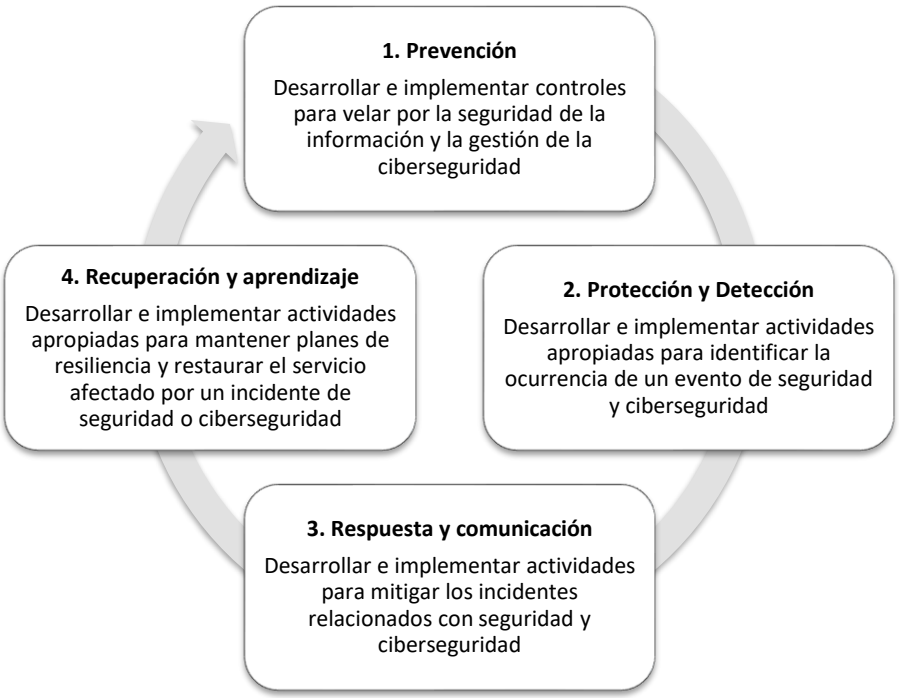
6. MEJORA CONTINUA MODELO DE SEGURIDAD DE FINDETER

El modelo de seguridad de la información de FINDETER, dentro de un proceso de mejora continua, se ha venido fortaleciendo mediante la adopción de mejorar prácticas de seguridad y la implementación de requerimientos que al respecto han establecido organismos de control y el Gobierno Nacional.

Las siguientes son las acciones más relevantes que se han implementado para la mejora continua del modelo de seguridad de la información de FINDETER:

ACCIONES 2018 Y 2019

Durante el 2018 y 2019, FINDETER fortaleció su modelo de seguridad mediante la implementación de los requerimientos para la gestión de la seguridad de la información y ciberseguridad establecidos por la Superintendencia Financiera de Colombia en la Circular Externa 007 de 2018. Para tal efecto, se implementaron y/o fortalecieron las siguientes fases:



Fase Implementación CE007/2018 SFC

ACCIONES 2020

- **Seguridad de la información en tiempos de COVID-19.** En el 2020, ante la crisis originada por la emergencia sanitaria del COVID-19, FINDETER adopto e implemento una serie de medidas administrativas, operativas y tecnológicas orientadas a habilitar y permitir el trabajo en casa y por ende el acceso remoto de los colaboradores a los servicios tecnológicos de la entidad. Lo anterior, trajo consigo un aumento en la probabilidad de ocurrencia e impacto de ataques cibernéticos que pueden afectar la ciberseguridad de la entidad y la normal operación y continuidad del negocio. Así mismo, se aumentó el nivel de exposición y de riesgo frente a fugas o robo de información personal o institucional, ataques de ingeniería social, accesos no autorizados, materialización de virus, fraudes y la posibilidad de explotación por parte de los ciberdelincuentes de las vulnerabilidades tecnológicas que lleguen a presentar los computadores que se utilizan en casa.

  Con el objetivo de gestionar de forma adecuada y oportuna los riesgos asociados al esquema de trabajo en casa y accesos remotos, FINDETER atendió los diferentes lineamientos de seguridad de trabajo en casa dados por la SFC y MINTIC.

- **Cumplimiento requerimientos CE033/2020 SFC.** Durante el último trimestre del 2020, se implementaron una serie de requerimientos de taxonomía y manejo de incidentes de seguridad de la información establecidas en la Circular Externa 033 de 2020 de SFC, relacionados con:
  - El uso del protocolo de etiquetado para el intercambio de información TLP (Traffic Light Protocol) y la taxonomía Única de incidentes (TUIC).
  - Clasificación de las categorías de los eventos de seguridad de la información.

ACCIONES 2021

- Fortalecimiento de la integración de incidentes de seguridad con los eventos de riesgos, lo que permitió la debida identificación y tratamiento de situaciones que atentaron contra la seguridad de la información de la entidad, lo anterior en cumplimento a lo establecido en la CE033/2020 SFC.
- **Revisión boletines de seguridad de terceros**. Se continuó con la atención de los boletines de seguridad reportados por la Superintendencia Financiera de Colombia y por los organismos que hacen parte del modelo nacional de gestión de ciberseguridad, con el objetivo de aplicar las recomendaciones y medidas de contención dadas por dichos organismos.
- **Atención Resolución No 00500 de marzo de 10 de 2021 de MinTIC**, que establece lineamientos y estándares para la estrategia de seguridad digital
- **Atención Directiva Presidencial No. 03 del Gobierno Nacional,** que establece lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.
- **Seguimiento de los riesgos generados durante la pandemia COVID-19**, con el objetivo de establecer y/o revisar la efectividad de los controles para mitigar dichos riesgos.

- **Certificación del SGSI de FINDETER en la Norma ISO 27001:2022**. FINDETER recibió por parte de SGS Colombia S.A.S, la certificación del Sistema de Seguridad de la Información SGSI en la norma ISO 27001:2022, producto de la auditoría externa realizada en los meses de noviembre y diciembre de 2021 para los procesos que soportan el alcance del sistema y que corresponde a "*Manejo de la información de las actividades relacionadas con la vinculación del cliente y la operación de los productos de Redescuento y Crédito Directo gestionados en la Sede Central. Basados en la Declaración de Aplicabilidad Versión 2 del 22 de noviembre de 2021*". Lo anterior, demuestra el compromiso de la entidad y la cultura de la mejora continua hacia la seguridad de la información y ciberseguridad de la organización y nos permite fortalecer la credibilidad y la imagen de la organización hacia nuestras partes interesadas.

ACCIONES 2022

- Continuamos con la gestión de los riesgos asociado a:
    - Riesgos que afectan la Disponibilidad, Integridad y Confidencialidad de la información.
    - Riesgos que afectan la seguridad de la infraestructura y servicios tecnológicos.
    - Riesgos de ciberseguridad.
    - Riesgos de seguridad digital.
    - Riesgos asociados al trabajo en casa, trabajo hibrido y accesos remotos.
    - Riegos de proveedores.
    - Riegos de servicios en la nube.
    - Riesgos que afectan la protección y privacidad de datos personales.

- **Programa Integral de Gestión de Protección de Datos Personales:** Se estableció un proyecto para el fortalecimiento del programa integral de gestión de datos personales de la entidad, que contempla el desarrollo de actividades que involucran la definición y actualización de roles, responsabilidades, políticas, procedimientos, controles, planes de formación y sensibilización, medición de indicadores y desempeño e informes para la debida gestión de los datos personales a los que Findeter tiene acceso y/o sobre los cuales figura como responsable de su tratamiento, de modo que puedan ser administrados de manera eficiente y clara, apoyados en directrices y procedimientos que garanticen su debida gestión y tratamiento de conformidad con la normativa aplicable y de acuerdo con los requerimientos del negocio.
- **Gestión de amenazas, eventos, incidentes, vulnerabilidades y boletines de seguridad de terceros**. Se continuó con la debida gestión de las amenazas, eventos, incidentes, vulnerabilidades y boletines de seguridad soportados. Estas labores se han venido fortalecimiento en la entidad debido a la debida gestión de los servicios de seguridad soportados en un SOC (Security Operation Center).
- **Circular Externa 018 de 2021 SFC.** Se estableció un proyecto para la implementación de la Circular Externa 018 de 2021 de la Superfinanciera de Colombia que establece los requerimientos para la implementación de un Sistema Integrado de Administración de Riesgos denominado SIAR.

- **Fortalecimiento de Controles.** Fortalecimos los controles de seguridad para la mitigación de riegos asociados a:
    - Uso de herramienta de mensajería
    - Intercambio de información institucional.
    - Acceso no autorizado. Se implemento del doble factor de autenticación
    - Robos de datos de autenticación. Se implementó mecanismo para la generación y almacenamiento seguro de contraseñas.
    - Acceso de proveedor. Se fortaleció los requerimientos técnicos y de seguridad para el acceso de los proveedores a los recursos tecnológicos de la entidad.

- **Auditorias de seguridad a los proveedores:** Se realizaron una serie de auditorías de seguridad a los proveedores con el objetivo de verificar sus niveles y medidas de seguridad y el debido cumplimiento de las obligaciones de seguridad de la información que se establecen en los contratos.
- **Certificación del SGSI de FINDETER en la Norma ISO 27001:2022**. FINDETER recibió por parte de SGS Colombia S.A.S, la recertificación de nuestro Sistema de Seguridad de la Información - SGSI en la norma ISO 27001:2022, producto de la auditoría externa de seguimiento realizada en el mes de noviembre de 2022 para los procesos que soportan el alcance del sistema y que corresponde a "*Manejo de la información de las actividades relacionadas con la vinculación del cliente y la operación de los productos de Redescuento y Crédito Directo gestionados en la Sede Central*.". Lo anterior, refuerza la integración de los procesos, demuestra el compromiso y la cultura de la mejora continua, fortalece la credibilidad y la imagen de la organización, y genera confianza entre nuestras partes interesadas, el Gobierno Nacional y los entes de control con relación a la aplicación de buenas prácticas en la organización en torno a la seguridad de la información y la ciberseguridad.

ACCIONES 2023

- **Gestión de amenazas, eventos, incidentes, vulnerabilidades y boletines de seguridad de terceros**. Se continuó con la debida gestión de las amenazas, eventos, incidentes, vulnerabilidades y boletines de seguridad soportados. Estas labores se han venido fortalecimiento en la entidad debido a la debida gestión de los servicios de seguridad soportados en un SOC (Security Operation Center).
- **Revisiones de seguridad a los proveedores:** Se ejecutaron las revisiones de seguridad a proveedores que proveen servicios críticos a la entidad con el fin de verificar el nivel de cumplimiento de las obligaciones de seguridad de la información y de ciberseguridad establecidas en los contratos.
- **Fortalecimiento cultura de Seguridad de la Información:** Se continuó con el fortalecimiento de la cultura organizacional de la entidad en torno a la seguridad de la información y ciberseguridad

por medio de campañas de socialización, sensibilización y capacitación que se llevaron a cabo de forma permanente.

- **Mejora Continua.** Con el fin de fortalecer y mejorar la gestión del SGSI, se gestionaron los hallazgos que fueron generados por revisiones tanto internas como externas efectuadas al sistema de gestión de seguridad de la información.
- **Proyecto Gestión de Identidad Fase II.** Se ejecutaron las actividades establecidas y se dio cierre al proyecto de Gestión de Identidades de acuerdo con cronograma establecido, logrando los objetivos propuestos para su desarrollo teniendo en cuenta las premisas, antecedentes y criterios de evaluación previamente considerados.
- **Proyecto Fortalecimiento Programa Integral de Datos Personales.** Se ejecutaron las actividades establecidas y se dio cierre al proyecto estructurado para fortalecer del programa integral de gestión de datos personales de la entidad de acuerdo con cronograma establecido, logrando los objetivos propuestos para su desarrollo teniendo en cuenta las premisas, antecedentes y criterios de evaluación previamente considerados.
- **Proyecto Transición Norma 21007 versión 2013 a versión 2022:** Se definió y estructuró un plan de transición para la actualización del Sistema de Gestión de Seguridad de la Información de acuerdo con los requisitos nuevos y modificados en la versión 2022 de la norma ISO 27001, que incluye actividades, responsables en la organización, temas clave, recursos requeridos y cronograma de ejecución.
- **Gestión de almacenamiento, administración y custodia de información Vicepresidencia Técnica:** Se presentaron los resultados generados sobre el plan de trabajo definido para poder establecer mecanismos a través de los cuáles se resuelvan y/o atiendan los problemas y necesidades de la Vicepresidencia Técnica en materia tecnológica, de seguridad de la información y de seguridad y salud en el trabajo, y que de una u otra forma, dificultan y/o limitan la ejecución de las actividades delegadas al proceso.
- **Fortalecimiento de la seguridad en la continuidad del negocio:** Se llevó a cabo un ejercicio teórico de simulación de un escenario de materialización de un ciberataque tipo Ransomware a través del cual se logró determinar, medir y comprobar la efectividad y eficacia de los procedimientos de comunicación, gestión de crisis, respuesta y gestión a incidentes de seguridad de la información y ciberseguridad que se tienen definidos en la entidad.
- **Actualización activos de información:** Se realizó el proceso de actualización de activos de información tanto en el sistema de administración de riesgos como en la página web de la entidad en cumplimiento a lo establecido en la Ley de transparencia y del derecho de acceso a la información pública nacional (Ley 1712 de 2014).
- **Fortalecimiento e implementación de controles:** Fortalecimos los controles de seguridad para la mitigación de riegos asociados a:

- ✓ **Fuga de Información:**
  - Configuración de DLP (Office 365)
  - Alertas nuevas sobre casos de uso para controlar salida de información por OneDrive y SharePoint
  - Control de navegación y uso de medios removibles a través de EDR (nueva plataforma de Endpoint)
- ✓ **Seguridad física:** Se definieron y documentaron nuevos controles para proteger las instalaciones, recurso humano y activos de información de la entidad de las amenazas externas; no solo limitando y controlando el acceso a la información, a la infraestructura y centros de almacenamiento y procesamiento, sino también previniendo el acceso físico no autorizado, el daño, pérdida, robo y/o fuga de información y de los activos que la contienen.
- ✓ **Gestión de Identidades:** Se fortaleció la gestión de identidades asociada a cuentas con altos privilegios, administradoras y de servicio.
- ✓ **Actualización de equipos:** Se implementó la política de apagada automática de equipos

- **Gestión de Riesgos:** Se continuo con la gestión de riesgos asociados a:
  - ✓ Riesgos que afectan la Disponibilidad, Integridad y Confidencialidad de la información.
  - ✓ Riesgos que afectan la seguridad de la infraestructura y servicios tecnológicos.
  - ✓ Riesgos de ciberseguridad.
  - ✓ Riesgos de seguridad digital.
  - ✓ Riesgos asociados al trabajo en casa, trabajo hibrido y accesos remotos.
  - ✓ Riegos de proveedores.
  - ✓ Riegos de servicios en la nube.
  - ✓ Riesgos que afectan la protección y privacidad de datos personales.

ACCIONES 2024

- **Gestión de amenazas, eventos, incidentes, vulnerabilidades y boletines de seguridad de terceros.** Se continuó con la debida gestión de las amenazas, eventos, incidentes, vulnerabilidades y boletines de seguridad soportados. Estas labores se han venido fortalecimiento en la entidad debido a la debida gestión de los servicios de seguridad soportados en un SOC (Security Operation Center).
- **Fortalecimiento seguridad de la información en la continuidad del negocio:** Se realizó a través de la definición de requisitos que son indispensables para la construcción de un marco de resiliencia y capacidad a través del cual se promueve una respuesta efectiva, adecuada y oportuna que permita reducir los daños potenciales que puedan ser ocasionados por un incidente de seguridad de la información y ciberseguridad que afecte o impacte la continuidad del negocio.
- **Revisiones de seguridad a los proveedores:** Se ejecutaron las revisiones de seguridad a proveedores que proveen servicios críticos a la entidad con el fin de verificar el nivel de cumplimiento de las obligaciones de seguridad de la información y de ciberseguridad establecidas en los contratos.

- **Fortalecimiento cultura de Seguridad de la Información:** Se continuó con el fortalecimiento de la cultura organizacional de la entidad en torno a la seguridad de la información y ciberseguridad por medio de campañas de socialización, sensibilización y capacitación que se llevaron a cabo de forma permanente y que fueron dirigidas a trabajadores, contratistas, proveedores y terceros con los que la entidad tiene algún tipo de relación.
- **Mejora Continua.** Con el fin de fortalecer y mejorar la gestión del SGSI, se gestionaron los hallazgos que fueron generados por revisiones tanto internas como externas efectuadas al sistema de gestión de seguridad de la información.
- **Programa Integral de Datos Personales:** Se continuó con el fortalecimiento y mejora del programa integral establecido para promover la debida gestión de los datos personales sobre los cuales Findeter tiene acceso y/o sobre los cuales figura como responsable de su tratamiento, a través de procesos y procedimientos que permiten fomentar su adecuada administración, apoyados en directrices y políticas que garanticen su debido tratamiento de conformidad con la normativa aplicable y en línea con los requerimientos del negocio.

- **Reporte Bases de Datos Personales:** Se reportaron ante el Registro Nacional de Bases de Datos de la SIC las bases de datos con información de índole personal sobre la cual Findeter figuras como responsable de su tratamiento.

- **Proyecto Transición Norma 21007 versión 2013 a versión 2022:** Se ejecutaron las actividades correspondientes de acuerdo con el cronograma y plan de trabajo definido y estructurado para la actualización del Sistema de Gestión de Seguridad de la Información teniendo en cuenta los requisitos nuevos y modificados en la versión 2022 de la norma ISO 27001.

- **Proyecto Implementación Controles Fuga de Información:** Se definió, estructuró y ejecutó parte del plan de trabajo y cronograma de actividades establecido para implementar controles que permitan detectar y prevenir la fuga de información, la transferencia o el uso indebido o no seguro de datos clasificados como restringidos o reservados en la entidad.
- **Actualización activos de información:** Se realizó el proceso de actualización de activos de información tanto en el sistema de administración de riesgos como en la página web de la entidad en cumplimiento a lo establecido en la Ley de transparencia y del derecho de acceso a la información pública nacional (Ley 1712 de 2014). Así mismo, se realizó la vinculación de los riesgos de seguridad de la información, ciberseguridad y datos personales con los activos de información identificados para cada proceso respectivamente.
- **Actualización Registros documentales:** Se realizó la actualización de 23 registros documentales y se crearon otros 13, entre procedimientos, documentos asociados, manuales y formatos para incorporar los requisitos nuevos y modificados por la nueva versión de la norma ISO 27001.

- **Revisiones independientes de seguridad de la información:** Se realizó pruebas de recorrido de controles y visitas de verificación físicas en las sedes de la entidad que incluyeron 4 de las regionales, con el objetivo de validar la implementación y operatividad de los controles de seguridad bajo las condiciones mínimas requeridas de acuerdo con lo establecido en el Manual de Políticas de Seguridad de la Información y Ciberseguridad de la entidad y a través de los cuales se soporta la gestión del SGSI.
- **Gestión de Riesgos:** Se continuo con la gestión de riesgos asociados a:
    - ✓ Riesgos que afectan la Disponibilidad, Integridad y Confidencialidad de la información.
    - ✓ Riesgos que afectan la seguridad de la infraestructura y servicios tecnológicos.
    - ✓ Riesgos de ciberseguridad.
    - ✓ Riesgos de seguridad digital.
    - ✓ Riesgos asociados al trabajo en casa, trabajo hibrido y accesos remotos.
    - ✓ Riegos de proveedores.
    - ✓ Riegos de servicios en la nube.
    - ✓ Riesgos que afectan la protección y privacidad de datos personales.

7. DOFA

Las Debilidades, Amenazas, Fortalezas y Oportunidades de Seguridad son identificadas en función de los riesgos y controles que se tienen implementados para gestionarlos y se alinean con el DOFA del Plan Estratégico de la Entidad.

Debilidades	Amenazas	Fortalezas	Oportunidades
Desconocimiento de las políticas de seguridad y la metodología de riesgos (D6)	Materialización de riesgos y amenazas cibernéticas por el uso indebido de los activos de información y de la información (A12)	Compromiso de la Alta Dirección para la implementación, establecimiento y mejorar continua del SGSI (F8)	Lograr la Certificación en la versión 2022 de la norma ISO/IEC 27001.
Desconocimiento de los usuarios para identificar amenazas de seguridad. (D6)	Expedición de nuevos requerimientos normativos cuya implementación sea compleja (A11)	Desarrollo y canales para las campañas de comunicación de los temas asociados a seguridad de la información.	Fortalecer la seguridad en procesos definidos en el alcance del SGSI ()
Recursos limitados para ejecutar y desarrollar actividades de seguridad. (D9)	Incremento de las amenazas cibernéticas que afectan la operación y continuidad de las entidades (A12)	Fortalecimiento del modelo de seguridad de la información y de ciberseguridad de la entidad al dar cumplimiento a las disposiciones normativas de los entes de control y del gobierno nacional (F8)	Promover el cumplimiento de las obligaciones de seguridad por parte de los proveedores
Debilidades en la revisión para el cumplimiento de los requerimientos de seguridad que se establecen en los contratos.	Tendencia creciente el uso de herramientas digitales no controlas por la entidad.	La entidad cuenta con una metodología integral para la gestión de riesgos operativos.	Adopción y fortalecimiento de las políticas de Seguridad de Información, estableciendo controles y normas para el manejo seguro de la información que permita aumentar la confianza de las partes interesadas.
Falencia en la implementación de controles o ausencia de estos.	Las condiciones de seguridad de los mecanismos de conectividad que usan en las casas para trabajo remoto.	Socialización de la gestión de seguridad de la información en varias instancias de la alta dirección de la entidad	Adopción de buenas prácticas de seguridad en ciclo de vida de desarrollo.

Debilidades	Amenazas	Fortalezas	Oportunidades
Falencias en los planes de recuperación ante la materialización de un ataque cibernético que afecte de forma crítica la continuidad del negocio.	Materialización de riesgos asociados a fuga de información debido al uso no controlado de herramientas de inteligencia artificial (A12)	Debida gestión de los eventos y riesgos que afecten la seguridad de la información y ciberseguridad de la entidad con el apoyo de un SOC.	Mitigación de riesgos que afecten la disponibilidad, integridad y confidencialidad de la información.
Insuficiencia en el control para el uso de herramientas de inteligencia artificial a nivel corporativo	Vulnerabilidades y brechas de seguridad sobre los sistemas e infraestructura tecnológica de la entidad (A12)	Contar con un Programa Integral de Protección de Datos Personales.	Apoyar la innovación y transformación digital asegurando la debida seguridad de la información es los respectivos proyectos que al respecto establezca la entidad.
Debilidades en el manejo de la información y repositorios de almacenamiento e intercambio de información (D2)	Pérdida de información y/o afectación de los sistemas de información por fallas o interrupción de los servicios esenciales de suministro causados por fenómenos climáticos extremos (cambio climático) (A9)	Contar con un Sistema de Gestión de Seguridad de la Información certificado en el estándar Normativo ISO 27001 (F2)	Lograr la debida y oportuna mitigación de vulnerabilidades.
Uso indebido de herramientas públicas y abiertas no autorizadas ni controladas por la entidad	Incremento de amenazas y eventos de seguridad a través de nuevas técnicas de ataque generadas bajo escenarios de crisis propiciados por desastres naturales (cambio climático) (A12)	Realizar revisiones permanentes de seguridad a los proveedores.	Definición de lineamientos para el uso e implementación de servicios en la nube de acuerdo con las regulaciones aplicables en esta materia y los riesgos derivados de estos servicios. (O2)
Falencia en la definición de una adecuada arquitectura integral para los servicios que se implementan en la nube		Contar con un Plan de Continuidad del Negocio y un Plan de Recuperación ante Desastres	Definición de lineamientos para el uso de herramientas de inteligencia artificial de acuerdo con las regulaciones aplicables en esta materia y los riesgos derivados de esta tecnología (O2)
No oportuna mitigación de las vulnerabilidades que se identifican sobre la infraestructura y		Realizar pruebas de continuidad que simulen escenarios de ataques cibernéticos para probar	

Debilidades	Amenazas	Fortalezas	Oportunidades
servicios tecnológicos de la entidad.		la efectividad de las estrategias y planes de respuesta y recuperación definidos por la entidad.	
		Contar con un Programa de Prácticas Sostenibles a través del cual se mitigan los efectos generados por el cambio climático (F8)	

8. MATRIZ RACI

La matriz RACI o matriz de asignación de responsabilidades, es una herramienta cuyo propósito es describir qué grado de responsabilidad tienen los diferentes recursos, personas, grupos y roles, frente a las diferentes procesos y actividades que soportan el Sistemas de Gestión de Seguridad de la Información de la Información.

Para la definición de la matriz RACI se establecen los siguientes actores:

R	Responsable	Encargado de hacer la tarea o actividad.
A	Aprobado	Responsable de que la tarea esté hecha. Es quién delega las tareas que deben ser ejecutadas en pro de realizar la tarea asignada a la persona responsable.
C	Consulado	Son todas aquellas personas las cuales brindan alguna información para la realización del trabajo. Son aquellos que brindan opiniones de valor.
I	Informado	Corresponde a quién se debe informar el estado o avance del desarrollo de la actividad

Las siguientes son las actividades relacionadas con la gestión de seguridad de la información y ciberseguridad y los actores o roles que intervienen en su ejecución, que apalanca el establecimiento, operación y mejora continua del Sistema de Gestión de Seguridad de la Información de la entidad:

Actividad	Rol								
	Junta Directiva	Comités asociados a seguridad	Oficial SI Vic. Riesgos	Unidades de Riesgos	Coordinador infraestructura Coordinador Aplicaciones	Responsable del Proceso	Gestor de Riesgos	Director Jurídico	Trabajador
Establecer manual de políticas de SI	A	I	R/A	R	C	I		C	
Actualizar el manual de SI			A/R	R	I	I			I
Establecer documentación para la gestión y operación del SGSI			A/R	R	R	R			
Establecer roles y responsabilidades de SI	A	A/R	C/I	I		I			
Socializar las políticas de SI			A/R	R		I			I
Diseñar y coordinar la implementación de las políticas de SI con la participación		I	A/R	R	I/R	I/R			I/R

Actividad	Rol								
	Junta Directiva	Comités asociados a seguridad	Oficial SI Vic. Riesgos	Unidades de Riesgos	Coordinador infraestructura Coordinador Aplicaciones	Responsable del Proceso	Gestor de Riesgos	Director Jurídico	Trabajador
activa de las áreas de para su debido cumplimiento.									
Establecer la metodología de gestión de riesgos SI.	A	I	A/R	R		I			
Identificar riesgos SI			A/R	R	R	R	R		R
Realizar análisis y evaluación de riesgos de SI			A/R	R		R/C	R		
Implementar plan de tratamiento de riesgos de SI			A/R	A/R	R	R/I	R		R/I
Definir guía para la gestión de eventos e incidentes de SI			A/R	R	I				
Monitorear y analizar las amenazas y eventos de SI y definir planes de tratamiento			A/R	R	R/I	R/I			
Implementar planes de tratamiento de eventos e incidentes de SI			A/R	A/R	R	R/I	R/I		R/I
Planear y ejecutar pruebas de vulnerabilidades y coordinar la ejecución de los respectivos planes de mitigación			A/R	R	R/I				
Mitigar vulnerabilidades tecnológicas			A	A	R				
Revisar a discreción la implementación de controles de seguridad establecidos.			A/R	A					
Definir lineamientos de desarrollo seguro y validar su aplicación			A/R	A	I				
Aplicar la seguridad en el ciclo de vida del software			A/C	A/C	R				
Definir instrumento para el levantamiento y clasificación de activos de información		I	R			I			
Realizar levantamiento y clasificación de activos de información		I	A/R	R	R	R			
Diseñar plan de capacitación y concientización en SI y Ciberseguridad		I	A/R	R		I			I
Implementar plan de capacitación y concientización		I	A/R	R		I			I
Atender auditorías internas y externas asociados a la SI y Ciberseguridad.		I	A/R	R	I/R	I/R			
Planear la continuidad de la seguridad de la información		I	A/R	R	C	C			
Definir componentes de seguridad para la continuidad del negocio			A/R	R	R/I				
Implementar medidas y de seguridad para BCP			A	A	R	R/I			
Realizar análisis de impacto del negocio			R/A	R	R/C				

Actividad	Rol								
	Junta Directiva	Comités asociados a seguridad	Oficial SI Vic. Riesgos	Unidades de Riesgos	Coordinador infraestructura Coordinador Aplicaciones	Responsable del Proceso	Gestor de Riesgos	Director Jurídico	Trabajador
Revisar y dar cumplimiento a la normatividad de seguridad aplicable a la entidad			R/A	R				C	
Establecer y actualizar la declaración de aplicabilidad			R/A	R	C	C			
Informar a la JD y los respectivos Comité la gestión de SI y ciberseguridad	I	I	R						

9. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025

Dependencia	Nombre de la tarea	Política de Gestión y Desempeño	Objetivo SGSI (*)	Responsable	Fecha Inicio	Fecha Fin	Fuente de Financiación
Vicepresidencia de Riesgos	Ejecución de campañas de sensibilización y socialización temas seguridad de la información y ciberseguridad al interior de la entidad	Seguridad Digital	OBJ 9	Grupo de Seguridad de la Información Dirección de Comunicaciones	1/01/2025	31/12/2025	Findeter $0
Vicepresidencia de Riesgos	Ejecución campañas de sensibilización y socialización temas seguridad de la información y ciberseguridad para clientes externos	Seguridad Digital	OBJ 9	Grupo de Seguridad de la Información Dirección de Comunicaciones	1/07/2025	31/12/2025	Findeter $0
Vicepresidencia de Riesgos	Ejecución campañas de sensibilización y socialización temas seguridad de la información y ciberseguridad para contratistas	Seguridad Digital	OBJ 9	Grupo de Seguridad de la Información Dirección de Comunicaciones	1/07/2025	31/12/2025	Findeter $0
Vicepresidencia de Riesgos	Actualizar el inventario de los activos de información de los procesos que soportan el alcance del SGSI cuando se presenten cambios	Seguridad Digital	OBJ 8 OBJ 9	Grupo de Seguridad de la Información Procesos	1/01/2025	31/12/2025	Findeter $0
Vicepresidencia de Riesgos	Realizar revisión de los riesgos de Seguridad de la Información, Ciberseguridad y Datos Personales y su vínculo con los activos de información.	Seguridad Digital	OBJ 8 OBJ 9	Grupo de Seguridad de la Información Procesos	1/01/2025	31/12/2025	Findeter $0
Vicepresidencia de Riesgos	Actualizar los registros documentales que soportan la gestión del SGSI y el Programa Integral de Protección de Datos Personales	Seguridad Digital	OBJ 8 OBJ 9	Grupo de Seguridad de la Información	1/01/2025	31/12/2025	Findeter $0
Vicepresidencia de Riesgos	Realizar pruebas de recorrido para verificar la implementación y operatividad de los controles de SIyC	Seguridad Digital	OBJ 8	Grupo de Seguridad de la Información	1/01/2025	31/12/2025	Findeter $0
Vicepresidencia de Riesgos	Atender los hallazgos resultado de las auditorías internas sobre el SGSI y externa de certificación de la ISO 27001	Seguridad Digital	OBJ 8 OBJ 9 OBJ 10	Grupo de Seguridad de la Información	1/01/2025	31/12/2025	Findeter $0
Vicepresidencia de Riesgos	Ejecutar proyecto Transición ISO 27001 V.2013 a V.2022	Seguridad Digital	OBJ 8 OBJ 9 OBJ 10	Grupo de Seguridad de la Información	1/01/2025	30/08/2025	Findeter $0
Vicepresidencia de Riesgos	Ejecutar proyecto Implementación Controles Fuga de Información	Seguridad Digital	OBJ 8 OBJ 9 OBJ 10	Grupo de Seguridad de la Información	1/01/2025	30/03/2025	Findeter $0
Vicepresidencia de Riesgos	Reportar ante el RNBD de la SIC las bases de datos con información de índole personal sobre la cual Findeter figure como responsable.	Seguridad Digital	OBJ 8	Grupo de Seguridad de la Información	1/01/2025	29/03/2025	Findeter $0
Vicepresidencia de Riesgos Dirección de Tecnología	Realizar pruebas que simulen escenarios de ciberataques, eventos y/o incidentes de seguridad	Seguridad Digital	OBJ 8 OBJ 9 OBJ 10	Grupo de Seguridad de la Información Dirección de Tecnología	1/01/2025	31/12/2025	Findeter $0

	que puedan afectar la continuidad del negocio y que involucren el componente tecnológico.						
Vicepresidencia de Riesgos	Reportar las cifras asociadas a la gestión de la Seguridad de la Información (incluyendo las relacionadas con Incidentes de Seguridad) a los entes de control y autoridades competentes	Seguridad Digital	OBJ 8 OBJ 10	Grupo de Seguridad de la Información	1/01/2025	31/12/2025	Findeter $0
Vicepresidencia de Riesgos	Verificar la implementación y operatividad de los controles de seguridad de la información en las sedes regionales de la entidad	Seguridad Digital	OBJ 8 OBJ 10	Grupo de Seguridad de la Información	1/07/2025	31/12/2025	Findeter $0
Vicepresidencia de Riesgos	Realizar la auditoría externa de certificación en la Norma ISO 27001:2022 que quedo pendiente del año 2024	Seguridad Digital	OBJ 8 OBJ 9 OBJ 10	Grupo de Seguridad de la Información Procesos del alcance 27001	1/01/2025	29/03/2025	Findeter $0
Vicepresidencia de Planeación Vicepresidencia de Riesgos	Realizar proceso de contratación del servicio de Auditoría interna sobre las Normas ISO 27001, 9001, 14000, 45000	Seguridad Digital	OBJ 8 OBJ 9 OBJ 10	Grupo de Seguridad de la Información Gerencia de Planeación y Gestión	01/04/2025	30/06/2025	Findeter $30.000.000
Vicepresidencia de Planeación Vicepresidencia de Riesgos	Realizar la auditoría interna sobre las Normas ISO 27001, 9001, 14000, 45000	Seguridad Digital	OBJ 8 OBJ 9 OBJ 10	Grupo de Seguridad de la Información Gerencia de Planeación y Gestión	30/06/2025	30/09/2025	Findeter $0
Vicepresidencia de Planeación Vicepresidencia de Riesgos	Realizar proceso de contratación de la auditoría externa de seguimiento a la certificación en Normas ISO 27001, 9001, 14000, 45000	Seguridad Digital	OBJ 8 OBJ 9 OBJ 10	Grupo de Seguridad de la Información Gerencia de Planeación y Gestión	1/07/2025	31/12/2025	Findeter $47.000.000
Vicepresidencia de Riesgos	Realizar valoración y revisiones de seguridad a los contratistas de la entidad de acuerdo con el plan anual establecido.	Seguridad Digital	OBJ 8	Grupo de Seguridad de la Información Supervisores	01/01/2025	31/12/2025	Findeter $0
Vicepresidencia de Riesgos	Realizar el monitoreo sobre la gestión de identidades de los aplicativos y sistemas de información de la entidad de acuerdo con el cronograma anual establecido	Seguridad Digital	OBJ 8	Grupo de Seguridad de la Información	1/01/2025	31/12/2025	Findeter $0
Vicepresidencia de Riesgos Dirección de Tecnología	Gestionar los eventos e incidentes de seguridad de la información y ciberseguridad	Seguridad Digital	OBJ 10	Grupo de Seguridad de la Información Dirección de Tecnología Proveedor de Seguridad	1/01/2025	31/12/2025	Findeter $ 900.610.802
Vicepresidencia de Riesgos Dirección de Tecnología	Realizar análisis de seguridad y/o vulnerabilidades	Seguridad Digital	OBJ 8 OBJ 10	Grupo de Seguridad de la Información Dirección de Tecnología	1/01/2025	31/12/2025	Findeter $240.000.000

(*) Objetivos del SGSI incluidos dentro del SGI
OBJ 8: Optimizar el nivel de efectividad de los controles de la Entidad.
OBJ 9: Incrementar el nivel de conciencia de los trabajadores en seguridad de la información para promover el uso adecuado de los activos de información.
OBJ 10: Fortalecer la seguridad de la información a través de la gestión oportuna de los incidentes y vulnerabilidades.

10. TERMINOS Y REFERENCIAS

Activo de información: aquello que es de alta validez y que contiene información vital de la empresa que debe ser protegida.

Amenaza: Es la causa potencial de un daño a un activo de información.

Anexo SL: Nuevo esquema definido por International Organization for Standardization - ISO para todos los Sistemas de Gestión acorde al nuevo formato llamado "Anexo SL", que proporciona una estructura uniforme como el marco de un sistema de gestión genérico.

Análisis de riesgos: Utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos.

Causa: Razón por la cual el riesgo sucede.

Cambio Climático: El cambio climático se refiere a la transformación a largo plazo de las condiciones meteorológicas de la Tierra. Este fenómeno está causado por una serie de factores tanto naturales como provocados por los seres humanos. Imagine que la Tierra es un invernadero gigante. Normalmente, el calor del sol entra y mantiene todo lo suficientemente caliente como para que vivamos cómodamente. Pero, cuando quemamos combustibles fósiles como el carbón, el petróleo y el gas para obtener energía, liberamos gases adicionales al aire. Estos gases atrapan más calor, con lo que nuestro «invernadero» es más cálido de lo que debería ser. Así, se desencadena el deshielo de los glaciares, la subida del nivel del mar y que fenómenos meteorológicos como huracanes y sequías se vuelvan más extremos y frecuentes.

Ciberseguridad: Es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de FINDETER. [CE 007 de 2018 SFC].

Ciclo de Deming: Modelo mejora continua para la implementación de un sistema de mejora continua.

Colaborador: Es toda persona que realiza actividades directa o indirectamente en las instalaciones de la entidad, Trabajadores de Planta, Trabajadores Temporales, Contratistas, Proveedores y Practicantes.

Confidencialidad: Propiedad que determina que la información no esté disponible a personas no autorizados

Controles: Son aquellos mecanismos utilizados para monitorear y controlar acciones que son consideradas sospechosas y que pueden afectar de alguna manera los activos de información.

Disponibilidad: Propiedad de determina que la información sea accesible y utilizable por aquellas personas debidamente autorizadas.

Dueño del riesgo sobre el activo: Persona responsable de gestionar el riesgo.

Impacto: Consecuencias de que la amenaza ocurra. Nivel de afectación en el activo de información que se genera al existir el riesgo.

Incidente de seguridad de la información: Evento no deseado o inesperado, que tiene una probabilidad de amenazar la seguridad de la información.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

Oficial de Seguridad: Persona encargada de administrar, implementar, actualizar y monitorear el Sistema de Gestión de Seguridad de la Información.

Probabilidad de ocurrencia: Posibilidad de que se presente una situación o evento específico.

PSE: Proveedor de Servicios Electrónicos, es un sistema centralizado por medio del cual las empresas brindan a los usuarios la posibilidad de hacer sus pagos por Internet.

Responsables del Activo: Personas responsables del activo de información.

Riesgo: Grado de exposición de un activo que permite la materialización de una amenaza.

Riesgo cibernético: Posibles resultados negativos derivados de fallas en la seguridad de los sistemas tecnológicos o asociados a ataques cibernéticos. [CE 007 de 2018 SFC].

Riesgo Inherente: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.

Riesgo Residual: Nivel de riesgo remanente como resultado de la aplicación de medidas de seguridad sobre el activo.

SARC: Siglas del Sistema de Administración de Riesgo Crediticio.

SARL: Siglas del Sistema de Administración de Riesgo de Liquidez.

SARLAFT: Siglas del Sistema de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo.

SARSICIB: Sistema de Administración de Riesgo de Seguridad de la Información y Ciberseguridad.

SARO: Siglas del Sistema de Administración de Riesgos Operativos.

Seguridad de la Información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información (ISO 27000:2014).

SGSI: Siglas del Sistema de Gestión de Seguridad de la Información.

Sistema de Gestión de Seguridad de la información SGSI: permite establecer, implementar, mantener y mejorar continuamente la gestión de la seguridad de la información de acuerdo con los requisitos de la norma NTC-ISO-IEC 27001.

Vulnerabilidad: Debilidad de un activo o grupo de activos de información que puede ser aprovechada por una amenaza. La vulnerabilidad de caracteriza por ausencia en controles de seguridad que permite ser explotada.