PLAN ANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION Y CIBERSEGURIDAD 2022

CÓDIGO: GR-DA-035
VERSIÓN 3
Clasificación: Público

Bogotá 19 de enero 2022

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
2022

Contenido

1. INTRODUCCION

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 27001:2013, 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 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 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 que la adicionen, modifiquen o substituyan.
- Entre otras.

El presente documento contiene el Plan de Seguridad de la Informacion y Ciberseguridad para el año 2021, 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.

2. OBJETIVO PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

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 2022 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. 6 y 8 SGI).

OE2. Fortalecer y optimizar la gestión de la seguridad de la información, seguridad digital y ciberseguridad al interior de FINDETER (Objetivo No. 8 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. 8 SGI).

OE4. Fortalecer la gestión integral de riesgos operativos que incluye los asociados a seguridad de la información y ciberseguridad (Objetivo No. 6 SGI)

OE5. Fortalecer la cultura de seguridad de la información y ciberseguridad en FINDETER (Objetivo No. 7 SGI).

OE6. Atender las observaciones, recomendaciones hallazgos de las auditorías internas y externas de control y vigilancia (Objetivos No. 6 y 8 SGI).

OE7. Atender los requerimientos de seguridad de la información, seguridad digital y ciberseguridad establecidos por el Gobierno Nacional y la SFC (Objetivos No. 6 y 8 SGI).

OE8. Mantener la certificación de la ISO 27001:2013 de acuerdo al alcancel de SGSI de la entidad. (Objetivos No. 6, 7 y 8 SGI).

3. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACION 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. METODOLOGIA ESTABLECIMIENTO MODELO DE SEGURIDAD

4.1. 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]:

Figura 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 Informacion 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.

4.2. ALINEACION NORMA ISO 27001:2013 VS CICLO DE OPERACION

Aunque en la norma ISO 27001:2013 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:

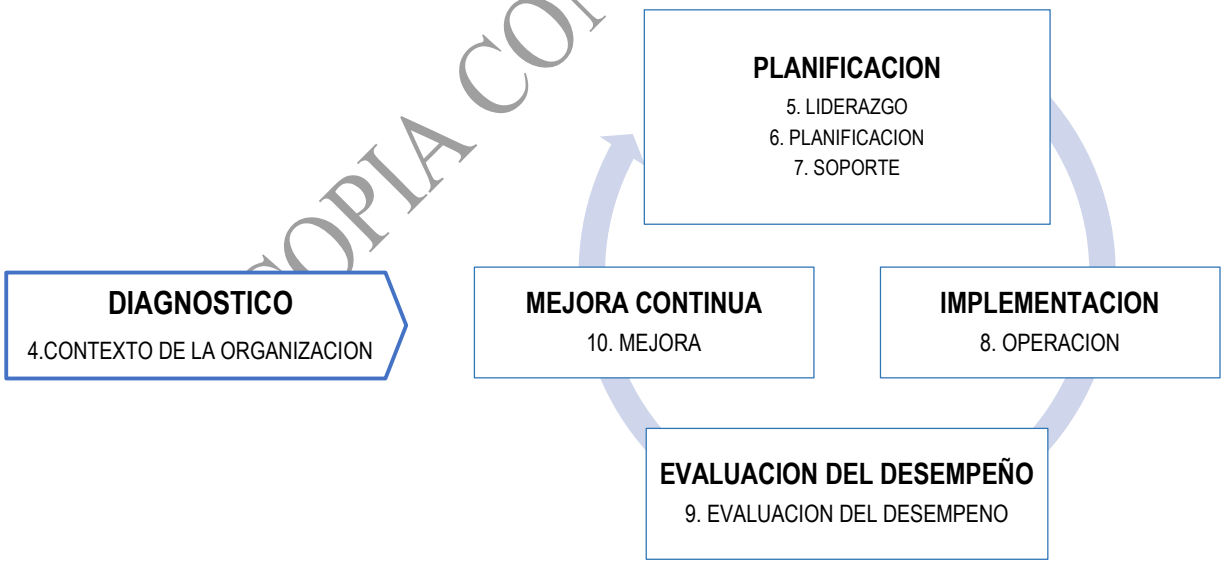

Figura 2. **Norma ISO 27001:2013 alineado al Ciclo de mejora continua**
Fuente: Elaborada con base en la información publicada en la página web *http://www.welivesecurity.com/la-es/2013/10/09/publicada-iso-270002013-cambios-en-la-norma-para-gestionar-la-seguridad-de-la-informacion/*

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 27001:2013:

Tabla 1. Fases Ciclo Operación vs Estructura ISO 27001:2013

Fase	Capitulo ISO 27001:2013[2]
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 DIAGNOSTICO en la norma ISO 27001:2013.** En el **capítulo 4 - Contexto de la organización** de la norma ISO 27001:2013, 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 PLANEACION en la norma ISO 27001:2013.** 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 IMPLEMENTACION en la norma ISO 27001:2013.** En el **capítulo 8 - Operación** de la norma ISO 27001:2013, se indica que la organización debe planificar, implementar y

[2] NTC-ISO-IEC 27001:2013, Pág. 1-12

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 EVALUACION DEL DESEMPEÑO en la norma ISO 27001:2013.** 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 27001:2013.** 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.

4.3. FASES I: DIAGNOSTICO

Objetivo	Identificar el estado de la Entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información

Figura 3. **Fase de diagnóstico modelo de seguridad**
Fuente: Documento Modelo de Seguridad y Privacidad de la Información estrategia de Gobierno en Línea

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. **Diagnostico nivel de cumplimiento** de la entidad frente a los objetivos de control y controles establecidos en el Anexo A de la **norma ISO 27001:2013**.

	Valoración estado actual de la gestión de seguridad de la entidad con base en el Instrumento de Evaluación MSPI de MINTIC.
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.

Para la recolección de la información, en esta fase se utilizarán mecanismo como:

- Diligenciamiento de cuestionarios con el objetivo de determinar el nivel de cumplimiento de le entidad con relación a los dominios de la norma ISO/IEC 27001:2013.
- Documentación existente en el sistema de calidad de la entidad relacionada con la información de las partes interesadas de la entidad y los roles y funciones asociados a la seguridad de la información.
- Fuentes externas, como las guías de autoevaluación, encuesta y estratificación dispuestas por la estrategia de gobierno en línea Ministerio de Tecnologías de la Información y las Comunicaciones.

4.4. FASES II: PLANIFICACION

Objetivo	Definir la estrategia metodológica, que permita establecer 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.

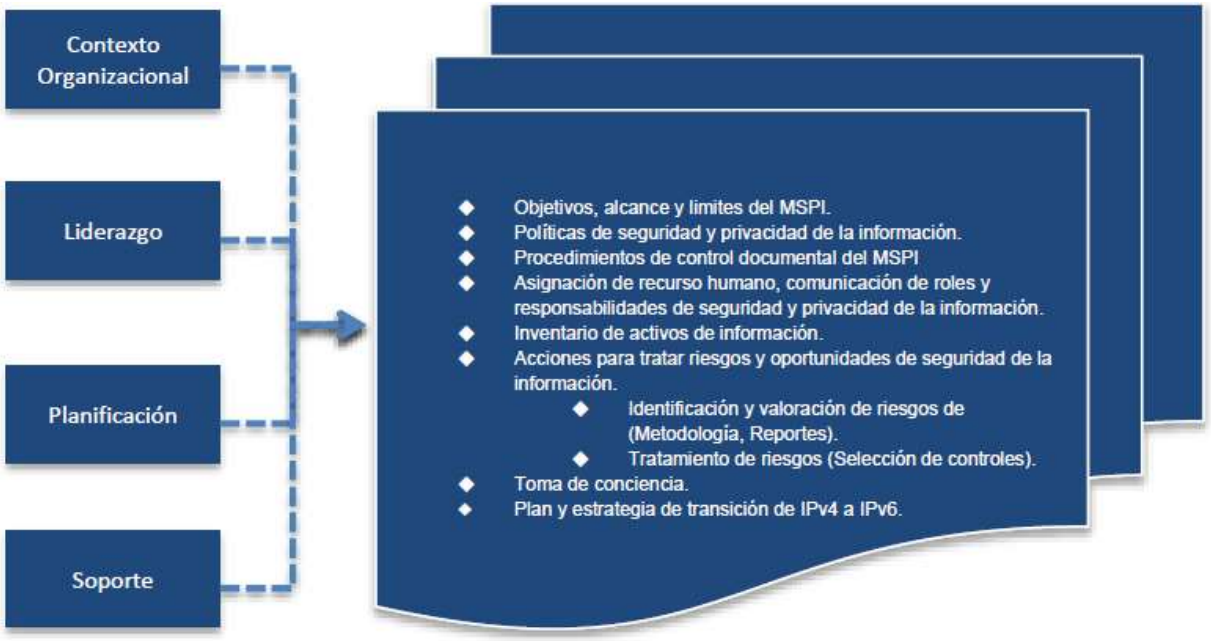

Figura 4. **Fase de planificación modelo de seguridad**
Fuente: Documento Modelo de Seguridad y Privacidad de la Información estrategia de Gobierno en Línea

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.	**Realizar** un **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 27001:2013, 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 (SGI).
Definir el alcance del SGSI de la entidad	**Definir** el **alcance** del **Sistema de Gestión de Seguridad de la Información** de la entidad aprobado por la Alta Dirección y socializado al interior de la Entidad (SGI). Definir el alcance del Sistema de Gestión de Seguridad de la Información, en el cual se establece los límites y la aplicabilidad del sistema.
Definir Roles, Responsables y Funciones de seguridad y privacidad de la información	**Adicionar** las **funciones de seguridad** de la información al **Comité de Riesgos** de la entidad y formalizarlas mediante acto administrativo. **Establecer** el **Rol** de **Oficial de Seguridad** de la información. **Definir** un **marco de gestión que contemple roles y responsabilidades** para la implementación, administración, operación y gestión de la seguridad de la información en la entidad.

	Definir la estructura organizacional de la Entidad que contendrá los roles y responsabilidad **pertinentes a la seguridad** de la información (SGI).
Definir la metodología de riesgos de seguridad de la información	**Definir Metodología** de Valoración de **Riesgos de Seguridad**. **Integrar** la **metodología** definida con la metodología de riegos operativos de la entidad (SGI). **Implementar** un **sistema de información** para la administración y gestión de los riesgos de seguridad de la entidad (SARI).
Elaborar las políticas de seguridad y privacidad de la información de la entidad	**Elaborar Política General de Seguridad y Privacidad** la cual debe ser aprobada por la Alta Dirección y socializada al interior de la Entidad (SGI). **Elaborar** el **manual de Políticas de Seguridad y Privacidad de la Información**, que corresponde a un documento que contiene las políticas y los lineamientos que se implementaran en la Entidad con el objetivo de proteger la disponibilidad, integridad y confidencialidad de la información. Estas políticas deben ser aprobadas por la Alta Dirección y socializadas al interior de la Entidad (SGI).
Elaborar documentación de operación (formatos de procesos, procedimientos y documentos debidamente definidos y establecidos) del sistema de seguridad de la información	**Elaborar** los **documentos de operación del sistema de seguridad** de la información, tales como: • Declaración de aplicabilidad (SGI). • Procedimiento y/o guía de identificación y clasificación de activos de información (SGI). • Procedimiento Continuidad del Negocio, Procedimientos operativos para gestión de TI (SGI). • Procedimiento para control de documentos (SGI) • Procedimiento para auditoría interna (SGI) • Procedimiento para medidas correctivas (SGI) • Procedimiento para la gestión de eventos e incidentes de seguridad de la información (SGI). • Procedimiento para la gestión de vulnerabilidades de seguridad de la información (SGI). • Entre otros.
Identificar y valorar activos de información	**Realizar** la **identificación** y **valoración** de los **activos de información** de la entidad de acuerdo con su nivel de criticidad de acuerdo con el alcance del modelo de seguridad. Documentar el inventario de los activos de información de la entidad.
Identificar, valorar y tratar los riesgos de seguridad de la información de la entidad	**Realizar** la **identificación** y **valoración** de los **riesgos** transversales de **seguridad** de la información y definir los respectivos planes de tratamiento. Realizar la valoración de riesgos de seguridad de la información y ciberseguridad. Definir los planes de acción que incluya los controles a implementar con el objetivo de mitigar los riesgos identificados en el proceso de valoración

	de riesgos. Para la seleccionar de los controles, se tomará como base los objetivos de control y los controles establecidos en el Anexo A de la norma ISO/IEC 27001:2013.
Establecer plan de capacitación, comunicación y sensibilización de seguridad de la información.	**Elaborar plan** anual de **capacitación** y sensibilización anual de seguridad de la información y ciberseguridad.
Establecer Plan de diagnóstico de IPv4 a IPv6	**Realizar** el **diagnóstico** para la **transición** de la entidad de **IPv4 a IPv6**. Documentar el Plan de diagnóstico para la transición de IPv4 a IPv6.

4.5. FASES III: IMPLEMENTACION

Objetivo	Llevar acabo la implementación de la fase de planificación del SGSI, teniendo en cuenta para esto los aspectos más relevantes en los procesos de implementación del Sistema de Gestión de Seguridad de la Información de la entidad.

Figura 5. **Fase de implementación modelo de seguridad**
Fuente: Documento Modelo de Seguridad y Privacidad de la Información estrategia de Gobierno en Línea

Metas	Actividades \ Instrumentos \ Resultados
Establecer el plan de implementación de seguridad de la información	**Implementar** el **plan de implementación** del **modelo de seguridad y privacidad** de la información el cual debe ser revisado y aprobado por el comité de riesgos
Ejecutar el plan de tratamiento de riesgos	**Ejecutar** el **plan de tratamiento de los riesgos** transversales de seguridad de la información identificados en la fase de planificación que fue presentado en el comité de riegos.
Ejecutar del plan y estrategia de transición de IPv4 a IPv6.	**Ejecutar plan de transición a IPv6** y elaborar informe de implementación.
Establecer indicadores de gestión de seguridad	**Definir los indicadores** para medir la gestión del modelo de seguridad y establecer los mecanismos para su medición. Estos indicadores deben permitir 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	**Implementar** el procedimiento y los mecanismos para la **gestión de los eventos e incidentes de seguridad** de la información**.**

Implementar procedimiento de gestión de vulnerabilidades	**Implementar** el procedimiento y los mecanismos para la **gestión de vulnerabilidades seguridad** de la información**.**
Ejecutar plan de capacitación y sensibilización de seguridad	**Ejecutar** el plan anual de capacitación, socialización y sensibilización de seguridad de la información
Ejecutar pruebas anuales de vulnerabilidades e intrusión	**Ejecutar** el plan anual de **pruebas vulnerabilidades** e intrusión con el objetivo de identificar el nivel de protección de los activos de información de la entidad. Para tal efecto, se deberá tener 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 o la circular que las reemplacen.
Ejecutar pruebas de Ethical Hacking	**Ejecutar** pruebas anuales de **Ethical Hacking** orientadas a poder determinar los niveles de riesgo y exposición de la organización ante atacantes interno o externo que puedan a comprometer activos críticos de la entidad y con esto generar interrupción en los servicios, afectar la continuidad del negocio y/o acceder de forma no autorizada a la información sensible o clasificada de la entidad o de carácter personal de los trabajadores o terceros que laboren para la entidad.
Ejecutar pruebas de Ingeniera Social	**Ejecutar** pruebas anuales de **ingeniería social** orientadas a verificar aspectos como: (i) los protocoles 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.

4.6. FASES IV: EVALUACION DE DESEMPEÑO

Objetivo	Evaluar el desempeño y la eficacia del SGSI, a través de instrumentos que permita determinar la efectividad de la implantación del SGSI.

Figura 6. **Fase Evaluación Desempeño modelo de seguridad**
Fuente: Documento Modelo de Seguridad y Privacidad de la Información estrategia de Gobierno en Línea

Metas	Actividades \ Instrumentos \ Resultados
Ejecución de auditorías de seguridad de la información	**Ejecución de 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 deberán llevar a cabo para la revisión del 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 27002:2013.
Plan de seguimiento, evaluación y análisis de SGSI	**Elaboración documento** con el **plan de seguimiento, evaluación y análisis del modelo de seguridad** revisado y aprobado por el Comité de Riesgos.

4.7. FASES V: MEJORA CONTINUA

Objetivo	Consolidar los resultados obtenidos del componente de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, que permita realizar el plan de implementación de las acciones correctivas identificadas para el modelo de seguridad.

Figura 7. **Fase Mejora Continua modelo de seguridad**
Fuente: Documento Modelo de Seguridad y Privacidad de la Información estrategia de Gobierno en Línea

Metas	Actividades \ Instrumentos \ Resultados
Diseñar plan de mejoramiento	**Diseñar** el **plan de mejoramiento continuo de seguridad** y privacidad de la información, que permita realizar el plan de implementación de las acciones correctivas identificadas para el Sistema de Gestión de Seguridad de la Información.

5. 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 mas 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 las siguientes fases:

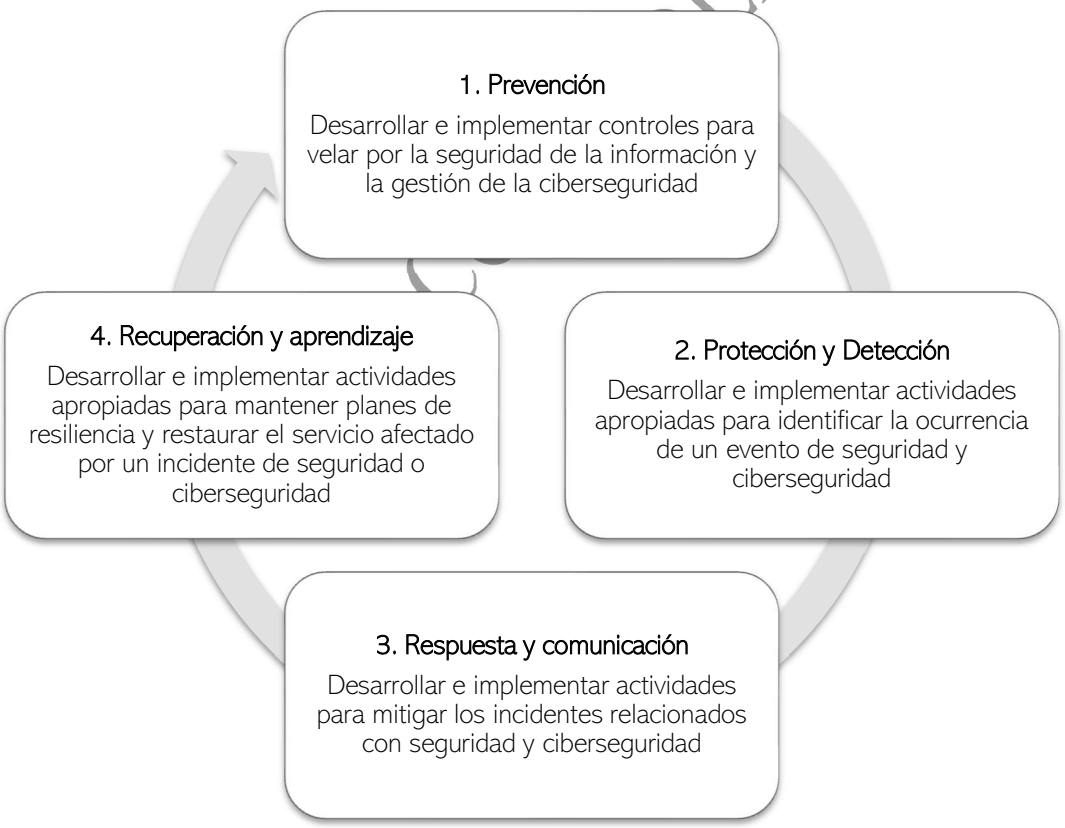

Figura 8. **Fase Implementación CE007/2018 SFC**

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 27001:2013**. FINDETER recibió por parte de SGS Colombia S.A.S, la certificación del Sistema de Seguridad de la Información SGSI en la norma ISO 27001:2013, 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.

6. DOFA

Debilidades	Amenazas	Fortalezas	Oportunidades
Desconocimiento de las políticas de seguridad y la metodología de riesgos	Materialización de riesgos y amenazas cibernéticas por el uso indebido de los activos de información y de la información (A2)	Compromiso de la Alta Dirección para la implementación, establecimiento y mejorar continua del SGSI (F2)	Certificación ISO/IEC 27001:2013
Desconocimiento de los usuarios para identificar amenazas de seguridad	Expedición de nuevos requerimientos normativos cuya implementación sea compleja (A3)	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	Incremento de las amenazas cibernéticas generadas por la pandemia del COVID-19 (A2)	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. (F1)	Fortalecer la aplicación de los controles seguridad con los proveedores.
Requerimiento de seguridad insuficientes en los contratos que se establecen con los terceros	Tendencia creciente el uso de herramientas digitales no controlas por la entidad.	La entidad cuenta con una metodología integral 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. (O8)
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. (A3)	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. (O7)

Debilidades	Amenazas	Fortalezas	Oportunidades
Capacidad de la entidad para la implementación de un SOC en cumplimiento a lo establecido por la SFC		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.	Reducción de riesgos que afecten la disponibilidad, integridad y confidencialidad de la información.
			Apoyar la innovación y transformación digital asegurando la debida seguridad de la información es los respectivos proyectos que al respecto establezca la entidad. (O7)

7. 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 Desarrollo	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 activa de las áreas de para su debido cumplimiento.		I	A/R	R	I/R	I/R			I/R
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			

Actividad	Rol								
	Junta Directiva	Comités asociados a seguridad	Oficial SI Vic. Riesgos	Unidades de Riesgos	Coordinador infraestructura Coordinador Desarrollo	Responsable del Proceso	Gestor de Riesgos	Director Jurídico	Trabajador
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				
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						

8. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2022

Dependencia	Nombre de la tarea	Política de Gestión y Desempeño	Objetivo SGSI (*)	Responsable	Fecha Inicio	Fecha Fin	Fuente de Financiación
Vicepresidencia de Riesgos Dirección de Comunicaciones	Sensibilización y socialización temas de seguridad de la información y ciberseguridad al interior de la entidad	Seguridad Digital	OBJ 7	Oficial de Seguridad de la Información Dirección de Comunicaciones	1/01/2022	31/12/2022	Findeter $0
Vicepresidencia de Riesgos Dirección de Comunicaciones	Ejecución campañas seguridad de la información y ciberseguridad para clientes externos	Seguridad Digital	OBJ 7	Oficial de Seguridad de la Información Dirección de Comunicaciones	1/07/2022	31/12/2022	Findeter $0
Vicepresidencia de Riesgos	Capacitar en temas de seguridad de la información a los proveedores que brindan servicios críticos para la entidad	Seguridad Digital	OBJ 7	Oficial de Seguridad de la Información	1/02/2022	31/12/2022	Findeter $0
Vicepresidencia de Riesgos	Actualización activos de información procesos alcance SGSI	Seguridad Digital	OBJ 6	Oficial de Seguridad de la Información Dueños de los procesos	1/02/2022	30/01/2022	Findeter $0
Vicepresidencia de Riesgos	Socializar en la entidad la guía para la identificación y valoración de activos de información y capacitar a los procesos con el fin de fortalecer el concepto de activo de información, sus tipos, como se clasifican.	Seguridad Digital	OBJ 7	Oficial de Seguridad de la Información	1/04/2022	30/07/2022	Findeter $0
Vicepresidencia de Riesgos	Capacitar a los procesos que soportan el alcance del SGSI en el manejo y concepto de activos de información	Seguridad Digital	OBJ 7	Oficial de Seguridad de la Información	1/07/2022	30/07/2022	Findeter $0
Vicepresidencia de Riesgos Vicepresidencia de Planeación	Actualización procedimiento de control de documentos y registros del SGI para incluir revisión de activos de información.	Seguridad Digital	OBJ 6	Oficial de Seguridad de la Información Gerencia de Planeación	1/03/2022	30/03/2022	Findeter $0
Vicepresidencia de Riesgos Vicepresidencia de Planeación	Asegurar que en el programa de la Auditoria Interna 2022 se incluyan todos los procesos que soportan el alcance del SGSI.	Seguridad Digital	OBJ 6	Oficial de Seguridad de la Información Gerencia de Planeación	1/07/2022	30/08/2022	Findeter $0
Vicepresidencia de Riesgos Vicepresidencia de Planeación	Capacitación a los auditores internos en el Sistema de Gestión de Seguridad de la Información.	Seguridad Digital	OBJ 8	Oficial de Seguridad de la Información Gerencia de Planeación	01/05/2022	30/06/2022	Findeter $0

Dependencia	Nombre de la tarea	Política de Gestión y Desempeño	Objetivo SGSI (*)	Responsable	Fecha Inicio	Fecha Fin	Fuente de Financiación
Vicepresidencia de Riesgos	Recertificación normas ISO 14001, 9001 y 27001	Seguridad Digital	OBJ 6 OBJ 7 OBJ 8	Vicepresidencia de Riesgos Gerencia de Planeación	1/06/2022	30/12/2022	Findeter $25.000.000
Vicepresidencia de Riesgos	Incluir requerimientos de seguridad de la información en el nuevo contrato del proveedor de custodia	Seguridad Digital	OBJ 6	Oficial de Seguridad de la Información	1/01/2022	30/04/2022	Findeter $0
Vicepresidencia de Riesgos Dirección de Contratación	Revisión de las directrices para incluir requerimientos de seguridad de la información en los contratos	Seguridad Digital	OBJ 6	Oficial de Seguridad de la Información Dirección de Contratación	1/02/2022	30/03/2022	Findeter $0
Vicepresidencia de Riesgos	Capacitar a los supervisores de contrato sobre la forma de asegurar y hacer seguimiento al cumplimiento de los requerimientos de seguridad de la información para los contratos que aplique.	Seguridad Digital	OBJ 7	Oficial de Seguridad de la Información Unidad de Riesgos Operativos	1/07/2022	30/07/2022	Findeter $0
Vicepresidencia de Riesgos Jefatura Servicios Generales	Realizar auditoria de seguridad a realizar al proveedor de custodia	Seguridad Digital	OBJ 6	Oficial de Seguridad de la Información Jefatura Servicios Generales	1/01/2022	30/01/2022	Findeter $0
Vicepresidencia de Riesgos	Definición procedimiento y/o instructivo para ejecución de auditorias de seguridad de la información	Seguridad Digital	OBJ 6	Oficial de Seguridad de la Información	1/03/2022	30/07/2022	Findeter $0
Vicepresidencia de Riesgos Dirección de Tecnología	Revisión de la efectividad de las reglas de correlación de eventos de seguridad	Seguridad Digital	OBJ 8 OBJ 6	Oficial de Seguridad de la Información Dirección de Tecnología Proveedor de Seguridad	1/01/2022	30/03/2022	Findeter $0
Vicepresidencia de Riesgos Dirección de Tecnología	Gestionar los eventos e incidentes de seguridad de la información y ciberseguridad	Seguridad Digital	OBJ 8	Oficial de Seguridad de la Información Dirección de Tecnología Proveedor de Seguridad	1/01/2022	31/12/2022	Findeter $0
Dirección de Tecnología	Mitigación de las vulnerabilidades de la prueba anual del Q2 de 2021	Seguridad Digital	OBJ 8	Dirección de Tecnología	1/01/2022	28/02/2022	Findeter $0
Vicepresidencia de Riesgos	Ejecución análisis de vulnerabilidades primera prueba anual Q1-2022	Seguridad Digital	OBJ 8	Oficial de Seguridad de la Información	1/03/2022	30/03/2022	Findeter $38,901.500

Dependencia	Nombre de la tarea	Política de Gestión y Desempeño	Objetivo SGSI (*)	Responsable	Fecha Inicio	Fecha Fin	Fuente de Financiación
				Proveedor de Seguridad			
Dirección de Tecnología	Mitigación de vulnerabilidad de la prueba anual del Q1-2022	Seguridad Digital	OBJ 8	Dirección de Tecnología	1/04/2022	30/06/2022	Findeter $0
Vicepresidencia de Riesgos	Ejecución análisis de vulnerabilidades primera prueba anual Q2-2022	Seguridad Digital	OBJ 8	Oficial de Seguridad de la Información Proveedor de Seguridad	1/07/2022	30/08/2022	Findeter $38,901.500
Dirección de Tecnología	Mitigación de vulnerabilidad de la prueba anual del Q2-2022	Seguridad Digital	OBJ 8	Dirección de Tecnología	1/09/2022	31/12/2022	Findeter $0
Vicepresidencia de Riesgos	Ejecución Prueba de Hacking ético	Seguridad Digital	OBJ 8	Oficial de Seguridad de la Información Proveedor de Seguridad	1/07/2022	31/12/2022	Findeter $16,566,514
Vicepresidencia de Riesgos	Ejecución Prueba de Ingeniería Social	Seguridad Digital	OBJ 7	Oficial de Seguridad de la Información Proveedor de Seguridad	1/07/2022	31/12/2022	Findeter $14,081,537
Vicepresidencia de Riesgos	Actualizar la gestión de riesgos de proveedores en el sistema WRM	Seguridad Digital	OBJ 6	Oficial de Seguridad de la Información Unidad Riesgos Operativos	1/01/2022	07/30/2022	Findeter $0

(*) Objetivos del SGSI incluidos dentro del SGI

OBJ 6: Optimizar el nivel de efectividad de los controles de la Entidad.
OBJ 7: Incrementar el nivel de conciencia de los trabajadores en seguridad de la información para promover el uso adecuado de los activos de información.
OBJ 8: Fortalecer la seguridad de la información a través de la gestión oportuna de los incidentes y vulnerabilidades.

9. 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.

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].

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.

Responsables del Activo: Personas responsables del activo de información.

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

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.

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.

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.