EXTRACTO DEL MANUAL DEL SISTEMA INTEGRAL DE ADMINISTRACIÓN DE RIESGOS – SIAR

CÓDIGO: GR-MA-021
VERSIÓN: 4
CLASIFICACIÓN: Clasificada (C)

Bogotá D.C, 29 de agosto de 2023
Junta Directiva Ordinaria Acta No 417.

1. INTRODUCCIÓN

FINDTER cuenta con un Sistema de Gestión de Seguridad de la Información - SGSI certificado en la norma ISO 27001:2013, 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 – SIAR, 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, 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.

Lo anterior implica, que FINDETER requiere conocer el estado actual de sus activos de información, clasificarlos, priorizarlos y determinar su valor en caso de pérdida de información, y conocer los posibles riesgos que puedan afectar la seguridad y privacidad de la información y ciberseguridad del negocio y de esta forma determinar las medidas orientadas a minimizar el impacto en caso de presentarse la materialización de una amenaza. En la medida que se tenga una visión general de los riesgos que pueden afectar la seguridad de la información y la Ciberseguridad del negocio, FINDETER puede establecer controles y medidas efectivas, viables y transversales con el propósito de salvaguardar la disponibilidad, integridad y confidencialidad de su información, para lo cual, es necesario definir los lineamientos que se deben seguir para el análisis, evaluación y tratamiento de los riesgos que afectan de Seguridad de la Información y la Ciberseguridad del negocio.

El presente documento corresponde a un extracto del Manual del Sistema Integral de Administración de Riesgos – SIAR de Findeter y mediante el cual se hace una descripción general de la metodología de gestión de riesgos de la entidad.

2. OBJETIVO

Establecer los lineamientos del Sistema Integral de Administración de Riesgos (SIAR) y los componentes de este, que permitan su cumplimiento, a través de la identificación, medición, control, monitoreo y comunicación de los riesgos que puedan afectar el cumplimiento de los objetivos estratégicos, minimizando las pérdidas para la compañía y sus accionistas.

3. MARCO NORMATIVO

- **Ley 87 de 1993:** por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones.
- **Ley 1474 de 2011:** Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
- **Ley 1581 de 2012:** Por la cual se dictan disposiciones generales para la protección de datos personales.
- **Decreto 2555 de 2010:** Por el cual se recogen y reexpiden las normas en materia del sector financiero, asegurador y del mercado de valores y se dictan otras disposiciones.
- **Decreto 2641 de 2012:** Por el cual se reglamentan el artículo 73, Plan Anticorrupción y de Atención al Ciudadano, y el artículo 76, Oficina de Quejas, Sugerencias y Reclamos de la Ley 1474 de 2011.
- **Decreto 1377 de 2013:** Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- **Decreto 663 de 1993:** Por el cual se actualiza el Estatuto Orgánico del Sistema Financiero y se modifica su titulación y numeración.
- **Decreto 1083 de 2015:** Por el cual se actualiza el Modelo Estándar de Control Interno (MECI).
- **Capítulo IV Título I Parte I de la Circular Externa Básica Jurídica 029 de 2014:** Sistema de Control Interno. Las entidades vigiladas por la SFC, ya sean matrices o subordinadas, deben implementar o ajustar su SCI a los requisitos mínimos establecidos en el presente Capítulo, en forma tal que el mismo resulte acorde con el tamaño de su organización (en términos de número de empleados, valor de los activos e ingresos, recursos captados del público, número de sucursales o agencias, entre otros) y la naturaleza de las actividades propias de su objeto social, así como de las desarrolladas por cuenta de terceros, teniendo en cuenta la relación beneficio/costo.
- **Capítulo I Título II Parte I de la Circular Externa Básica Jurídica 029 de 2014:** Instrucciones generales aplicables a las entidades vigiladas. Canales, medios, seguridad y calidad en el manejo de información en la prestación de servicios financieros.
- **Capítulo V Título IV Parte I de la Circular Externa Básica Jurídica 029 de 2014:** Instrucciones generales aplicables a las entidades vigiladas. Requerimientos mínimos para la gestión de la seguridad de la información y la ciberseguridad.
- **Circular Externa 033 de 2014**: Catálogo único de información financiera con fines de supervisión.
- **Capítulo I – 1 de la Circular Externa Básica Contable y Financiera 100 de 1995:** Evaluación

de inversiones.

- **Capítulo XIII – 16 de la Circular Externa Básica Contable y Financiera 100 de 1995:** Margen de solvencia y otros requerimientos de patrimonio
- **Capítulo XVIII de la Circular Externa Básica Contable y Financiera 100 de 1995:** Instrumentos Financieros Derivados y Productos Estructurados
- **Capítulo XXXI de la Circular Externa Básica Contable y Financiera 100 de 1995:** Imparte instrucciones relacionadas con el Sistema Integral de Administración de Riesgos (SIAR).
- **Reglamento AMV:** Reglamento de Autorregulación aplicable a todos los intermediarios del mercado de valores miembros de AMV.
- **Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP:** El Departamento Administrativo de la Función Pública, como entidad técnica, estratégica y transversal del Gobierno nacional, pone a disposición de las entidades la metodología para la administración del riesgo.
- **NTC-ISO 9001:2015:** Esta norma internacional promueve la adopción de un enfoque a procesos al desarrollar, implementar y mejorar la eficacia de un sistema de gestión de la calidad, para aumentar la satisfacción del cliente mediante el cumplimiento de los requisitos del cliente.
- **NTC-ISO 14001:2015:** El propósito de esta norma Internacional es proporcionar a las organizaciones un marco de referencia para proteger el medio ambiente y responder a las condiciones ambientales cambiantes, en equilibrio con las necesidades socioeconómicas.
- **NTC-ISO-IEC 27001:2013:** Esta norma específica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información dentro del contexto de la organización.
- **Código de Buen Gobierno:** Con este Código Findeter establece el marco de acción para sus actuaciones de gobierno, con el propósito de fortalecer el mejoramiento permanente y planeado para una buena gestión, el uso adecuado de los recursos disponibles, mitigar los riesgos relacionados, mejorar la capacidad para la toma de decisiones y disminuir la existencia de conflictos entre las partes interesadas.
- **Reglamento para Operaciones de Redescuento:** Este reglamento define la política, los intermediarios, los beneficiarios, el uso de los recursos, los sectores financiables, las condiciones financieras, que aplican a la operación de redescuento de Findeter.
- **Reglamento para Operaciones de Crédito Directo:** Este reglamento tiene por objeto instrumentalizar las políticas, procesos, condiciones, criterios y metodologías, para atender el ciclo de crédito y la gestión del riesgo crediticio de las operaciones autorizadas a la Financiera de Desarrollo Territorial S.A. denominadas crédito directo.

4. GESTIÓN PARA LA ADMINISTRACIÓN INTEGRADA DE RIESGOS

Teniendo en cuenta que todas las actividades que realiza una organización generan riesgo, se establece la gestión del riesgo como una práctica gerencial fundamental que permite asegurar el logro de los objetivos estratégicos. De esta forma, el Sistema de Administración de Riesgos Integrados, que incluye los de seguridad de la información,seguridad digital y ciberseguridad, busca asegurar la operación de Findeter contenida en sus procesos, para un uso eficiente de los recursos a través del desarrollo de cada una de sus etapas y elementos, brindando información relevante para la toma de decisiones respecto a la gestión de riesgos asociada a la operación de la Entidad.

A continuación, se describe de forma general la metodología y cada una de las etapas para la administración en la gestión del riesgo operacional, que incluye los riesgos de seguridad de la información, seguridad digital y ciberseguridad, los cuales se desarrollan a través de los procedimientos, instructivos, herramientas tecnológicas y demás mecanismos que se estimen pertinentes para su aplicación.

5. METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO OPERACIONAL

El modelo a través del cual se desarrolla la implementación del sistema dentro de FINDETER se presenta a continuación:

Fuente: Manual SIAR de Findeter

Bajo el criterio que la gestión de riesgos debe ser un instrumento que contribuya al logro de los objetivos de Findeter, la identificación del riesgo se apoya en el contexto estratégico definido por la Alta Dirección y la Junta Directiva.

Una vez establecidos los objetivos estratégicos, se identifica a cuál o cuáles de estos se alinean los objetivos de los procesos, estableciendo de esta forma qué parte de la operación apalanca qué propósito estratégico. Una vez realizado este análisis, se inicia la identificación de riesgos por cada uno de los procesos contenidos en el mapa de procesos del Sistema de Gestión Integrado de FINDETER.

5.1 ETAPA DE IDENTIFICACIÓN

La identificación de los riesgos, incluidos los riesgos de seguridad y privacidad de la información, seguridad digital y ciberseguridad, los realiza el Líder del Proceso o quién este designe con el apoyo de la Unidades de Riesgo, quienes aportan la metodología para adelantar adecuadamente dicha identificación y documentación de los riesgos inherentes. Teniendo en cuenta lo anterior, la gestión del riesgo se basa en la identificación de riesgos desde los procesos, entendiendo que los procesos se alinean a los objetivos institucionales, es decir, que la operación se organiza para cumplir con la estrategia.

La identificación de los riesgos es la etapa fundamental del sistema ya que aquello que no se contemple en esta etapa será excluido de las demás. Esta parte de la identificación de los diferentes eventos que se puedan presentar o se hayan presentado en el desarrollo del proceso, independientemente de si está bajo el control o no de FINDETER pero que impacten en el logro de los objetivos.

Para adelantar una adecuada identificación del riesgo inherente en los procesos se deben tener en cuenta diferentes fuentes de información que pueden aportar lo necesario para prever tantos riesgos como sea posible. Con la información recabada de las diferentes fuentes de información las Unidades de Riesgos estructuran los riesgos del proceso y alimenta la matriz de riesgos.

Identificación y clasificación activos de información.

Un activo de información es todo aquel elemento que es vital para FINDETER o que por una disposición legal tiene dicho tratamiento, el cual debe ser protegido y asegurado con el objetivo de garantizar su disponibilidad, integridad y confidencialidad, debido a que a través de él se gestiona la información de la entidad.

En esta etapa de la gestión del riesgo, el Líder del Proceso o quién este designe con el apoyo de las Unidades de Riesgos, identifican y clasifican los activos de información involucrados en la gestión del proceso y activos de información críticos del negocio, sobre los cuales se determinan las causas (amenazas) y las fuentes (vulnerabilidades) que pueden afectar o exponer su seguridad con el propósito de que en la fase de control se identifiquen las medidas a implementar para proteger su disponibilidad, integridad y confidencialidad.

Para la identificación de los activos de información se tiene en cuenta todo aquel elemento o recurso por medio del cual se gestiona, protege, recolecta, administra, procesa, almacena, respalda o se distribuye la información del negocio. En esta etapa, los procesos deben realizar un inventario detallado de los activos de información que tienen a su cargo, bajo su custodia o que utilizan para el desarrollo de sus actividades laborales, para lo cual deben tener en cuenta la información contenida en la descripción de sus procesos.

Así mismo, se deben tener en cuenta los activos de información expuestos en el ciberespacio sobre los cuales se deben establecer medidas y controles especializados para su protección que permitan defenderse y anticiparse a las amenazas cibernéticas que puedan afectar la seguridad de FINDETER.

5.2 ETAPA DE MEDICIÓN

En primer lugar, se debe tener en cuenta que el riesgo se basa en la percepción de que algo pueda ocurrir, por tal razón tiene un carácter subjetivo. Su medición busca establecer criterios que permitan acercarse al riesgo de manera objetiva con el fin de priorizarlos para facilitar su gestión por parte de los Líderes de los Procesos.

La medición del riesgo se realiza a través de dos variables llamadas probabilidad e impacto. La probabilidad de ocurrencia del riesgo hace referencia a la posibilidad de que suceda algo en el desarrollo de la operación de la entidad y que afecte su desempeño. Esta variable tiene unos criterios asociados que permiten a los Líderes de los Procesos valorarla de acuerdo con su experiencia y conocimiento técnico.

La variable impacto busca determinar las consecuencias que podría llegar a generar la materialización de un riesgo en diferentes esferas. Para efectos de esta metodología se ha establecido que un riesgo puede tener consecuencias económicas, legales, reputacionales, de seguridad de la información y operacionales, de contagio y ambientales, según el tipo de riesgo.

El resultado de la combinación de estas variables permite la construcción del perfil de riesgo inherente, el cual se expresa a través del mapa de riesgos definido en la metodología de medición del riesgo integral.

Valoración activos de información

Una vez identificados los activos de información se deben valorar de acuerdo con su criticidad, necesidad, prioridad y nivel de protección. El objetivo es valorar cada activo de información de acuerdo con su grado de importación y criticidad para la organización, para lo cual se debe tener en cuenta:

- Los niveles de clasificación establecidos en el régimen de transparencia y acceso a la información: Información Reservada, Información Clasificada e Información Pública.
- La preservación de los tres principios fundamentales en los cuales se basa la seguridad de la información: disponibilidad, integridad y confidencialidad
- Las necesidades de compartir o restringir el acceso al activo de información.
- El impacto negativo que pudiera provocar al negocio en términos financieros, legales, de imagen u operacionales, en caso dado que al materializarse una amenaza afecte la seguridad del activo de información.
- Los requerimientos normativos vigentes y aplicables a la entidad y requerimientos legales de retención.

5.3 ETAPA DE CONTROL

El control consiste en una actividad o una validación manual o automática que busca mitigar la probabilidad o el impacto de uno o varios riesgos. Los controles se identifican y documentan en cada uno de los procedimientos, instructivos y guías que soportan la operación de FINDETER. Consisten en aquellas actividades específicas que resultan puntos clave donde se está validando que se cumplan con los criterios establecidos en el objetivo del proceso y del procedimiento en sí mismo.

Dado que un control puede mitigar uno o varios riesgos, es importante durante esta etapa asociarlo a los riesgos que contribuye a gestionar, por cuanto el apoyo de las Unidades de Riesgos al Líder del Proceso o a quien este designe resulta relevante, así como para la valoración de este. Así mismo, aquellos controles que mitiguen riesgos de seguridad de la información y ciberseguridad deben estar asociados a controles establecidos en la ISO 27001 o en marcos de referencia de buenas prácticas de seguridad que FINDETER haya decidido adoptar.

Cuando un control deje de mitigar el riesgo porque perdió efectividad el Líder del Proceso deberá tomar las medidas necesarias para que el proceso sea asegurado. De acuerdo con los riesgos que pueden afectar la seguridad y ciberseguridad de los activos de información, en esta fase se debe establecer los mecanismos adecuados para protegerlos contra amenazas internas, externas y provenientes del ciberespacio que puedan afectar su seguridad.

Una vez aplicado lo anterior se puede construir el perfil de riesgos neto de la organización.

5.4 ETAPA DE MONITOREO

Una vez mitigado el riesgo a través del establecimiento de controles, se debe ejercer monitoreo sobre éstos para asegurar que estén funcionando y que no pierdan efectividad frente a la gestión del riesgo.

Una de las principales herramientas de monitoreo es la supervisión continua que los Líderes de Proceso y Jefes de Área deben ejercer para verificar el desempeño de los controles, labor que pueden ejercer apoyándose en estadísticas que estos establezcan, así como en los indicadores de los procesos. Los planes de acción que contribuyan a la gestión del riesgo se constituyen en una herramienta de monitoreo, así como el respectivo seguimiento a la ejecución de sus actividades.

Por otra parte, el seguimiento efectuado por el SOC, las evaluaciones y auditorías realizadas por la Auditoría Interna, así como, las diferentes auditorías realizadas a FINDETER por los diferentes Entes de Control, son consideradas parte del seguimiento y monitoreo de la gestión del riesgo operacional, ya que estas permiten medir la efectividad de los controles establecidos.

Como mínimo semestralmente las Unidades de Riesgos realizarán el seguimiento a los tratamientos que gestionan los riesgos con el objeto de validar que se esté mitigando oportunamente. Esta información será incluida dentro del informe semestral del monitoreo al perfil de riesgo que se presenta al Representante Legal

y que este, a su vez presenta a la Junta Directiva.

La gestión del riesgo se ajustará como consecuencia de los eventos de riesgos e incidentes de seguridad presentados, adoptando los controles que resulten pertinentes. Esta información también será incorporada al informe semestral.

Tanto la matriz de riesgos como los controles asociados deben contar con mecanismos que permitan tener trazabilidad sobre su evolución, con el objeto de evidenciar la mejora del sistema en el tiempo.

5.5 METODOLOGÍA DE COMUNICACIÓN

Cada etapa de la Gestión Del Riesgo debe ser comunicada y consultada con los interesados, con el objeto de realizar una construcción colectiva del sistema que permita racionalizar esfuerzos en la gestión del riesgo. Para realizar una comunicación efectiva se debe considerar qué se comunicará, cuándo y a quiénes.

En la etapa de identificación la información debe ser recogida del Líder y/o sus designados, así como de las diferentes fuentes de información de las que se disponga. Una vez establecidos los riesgos, las Unidades de Riesgos deben informarlos al Líder del Proceso para que este pueda medirlos de acuerdo con los criterios definidos. Durante la etapa de control, el Líder del Proceso debe establecer los controles que gestionen los riesgos identificados.

Es deber de las Unidades de Riesgos informar al Líder si el control mitiga o no el riesgo, con el objeto de que este establezca las acciones necesarias. En este orden de ideas, tanto el Líder como la Alta Dirección deben conocer los resultados de las etapas de identificación, medición, control y monitoreo con el objeto de que se pueda tomar las decisiones a las que haya lugar.

Las Unidades de Riesgos deben proporcionar con la periodicidad establecida o cada que se le requiera, información suficiente tanto a los Líderes de Proceso como a la Alta Dirección, para que la toma de decisiones se base en información disponible de fuentes confiables.

5.6 METODOLOGÍA DE REGISTRO DE EVENTOS DE RIESGO.

El registro de eventos de riesgo el cual incluye los incidentes de seguridad permite contar con una base de datos de las situaciones ocurridas, la forma en la cual se solucionaron y las pérdidas económicas que causaron, convirtiéndose en una herramienta clave para la gestión del riesgo.

La base de datos es única en FINDETER y la información allí contenida es de carácter confidencial. Su uso estará enfocado primordialmente al análisis de las situaciones presentadas en los procesos y a la cuantificación del riesgo, de tal forma que le permita a la Organización mejorar sus procesos y las fallas presentadas en la ejecución de los mismos, en la medida que los eventos se clasifiquen correctamente, así como estimar posibles futuras pérdidas.

Las Unidades de Riesgos administrarán la base de datos a través de la herramienta tecnológica definida para este fin, así mismo, analizarán la información allí registrada por los trabajadores y generará informes periódicos. Dicha base de datos debe contener los campos mínimos requeridos por la norma, así como otros que se estimen convenientes para el análisis de los eventos.

Las Unidades de Riesgos podrá registrar los eventos de los que tenga conocimiento y que no hayan sido registrados por otro usuario con la información disponible, así mismo podrá modificar el registro de acuerdo con los análisis y revisiones que realice de cada caso.

Para la afectación contable de aquellos eventos de riesgo clasificados en el tipo a) "Generan pérdidas y afectan el estado de resultados de la entidad", se utilizarán las cuentas contables definidas por la SFC, en el Catálogo Único de Información Financiera CUIF respectivo, para lo cual el área contable, creará las cuentas en la herramienta tecnológica utilizada por FINDETER para el manejo contable de los estados financieros, así mismo, deberá mantener una constante supervisión sobre las cuentas marcadas como riesgo operacional.

Plataforma Tecnológica

Findeter cuenta con una plataforma tecnológica que le permite gestionar los riesgos a los cuales se ve expuesta en el desarrollo de su operación, así como el registro de los eventos materializados. Dicha plataforma.