Findeter
Banca de Desarrollo Territorial

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACION Y CIBERSEGURIDAD 2020

SISTEMA DE ADMINISTRACION DE RIESGOS DE SEGURIDAD DE LA INFORMACION Y CIBERSEGURIDAD
SARSICIB
VICEPRESIDENCIA DE RIEGOS
2020

TABLA DE CONTENIDO

1. INTRODUCCION

FINDETER ha establido un Sistema de Administración de Seguridad y Ciberseguridad de la Información – SARSICIB por medio del cual gestiona y administra los riesgos, eventos, amenazas, vulnerabilidades y situaciones que pueden afectar la seguridad de la información y ciberseguridad de FINDETER, lo anterior de acuerdo con los requerimientos del negocio y en cumplimiento de las disposiciones legales vigentes emitidas por la Superintendencia Financiera de Colombia - SFC y el Gobierno Nacional.

El objetivo primordial de este sistema es garantizar que los riesgos asociados a la seguridad de la información, seguridad digital y ciberseguridad sean conocidos, gestionados y tratados de forma documentada, sistemática, estructurada, repetible y eficiente.

Lo anterior implica, que FINDETER requiere como 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.

Para tal efecto, FINDETER ha diseñado una metodología integral de riesgos operativos, que incluye tanto los riesgos operativos como los riesgos asociados a la seguridad de la información, seguridad digital y ciberseguridad.

El Sistema de Administración de Riesgos de Seguridad de la Información y Ciberseguridad - SARSICIB contempla los requerimientos y lineamientos establecidos en la Circular Externa 007 de 2018 de la Superintendencia Financiera de Colombia, que imparte instrucciones relacionadas con los requerimientos mínimos para la gestión del riesgo de seguridad de la información y ciberseguridad que las entidades vigiladas deben cumplir.

El presente documento contiene entre otros aspectos, el plan de tratamiento de riesgos de seguridad de la informacion y ciberseguridad para el año 2020.

2. OBJETIVO

Definir un marco regulatorio interno que permita identificar, medir, tratar, controlar, monitorear y comunicar los riesgos operativos “incluido los de seguridad de la información, seguridad digital y ciberseguridad” asociados a la operación de FINDETER y que puedan afectar el cumplimiento de los objetivos estratégicos, minimizando las pérdidas para FINDETER y sus accionistas.

3. MARCO NORMATIVO

A continuación, se enuncian las normas que rigen la gestión del riesgo operativo:

- **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.
- **Decreto 943 de 2014:** Por el cual se actualiza el Modelo Estándar de Control Interno (MECI).
- **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 IV Título I Parte I de la Circular Externa Básica Jurídica 029 de 2014 - SFC:** 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 V Título IV Parte I de la Circular Externa Básica Jurídica 029 de 2014 - SFC:** Requerimientos mínimos para la gestión de la seguridad de la información y la ciberseguridad
- **Capítulo XXIII de la Circular Externa Básica Contable y Financiera 100 de 1995:** Reglas Relativas a la Administración del Riesgo Operativo. Todas las entidades sometidas a la inspección y vigilancia de la SFC deben adoptar un Sistema de Administración de Riesgo Operativo (SARO), con excepción de las Oficinas de Representación de instituciones financieras y reaseguradoras del exterior.
- **Resolución 1865 de 2007 de la SFC:** Por medio de la cual se incluyen cuentas para registrar el Riesgo Operativo en los planes únicos de cuentas (PUC) aplicables a las

entidades sometidas a inspección y vigilancia de la Superintendencia Financiera de Colombia obligadas a implementar el Sistema de Administración de Riesgo Operativo –SARO –.

- **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.
- **Decreto 2641 de 2012:** Por el cual se reglamentan el artículo 73, Plan Anticorrupción y de Atención al Ciudadano, y el artículo76, Oficina de Quejas, Sugerencias y Reclamos de la Ley 1474 de 2011.
- **Ley 872 de 2003:** Por la cual se crea el sistema de gestión de la calidad en la Rama Ejecutiva del Poder Público y en otras entidades prestadoras de servicios.
- **Decreto 4110 de 2004:** Por el cual se reglamenta la Ley 872 de 2003 y se adopta la Norma Técnica de Calidad en la Gestión Pública.
- **Código de Buen Gobierno de 2014:** 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.

4. METODOLOGIA PARA LA ADMINISTRACION INTEGRAL DE RIESGOS

FINDETER ha dado cumplimiento a las diferentes directrices de gestión de riesgos que la Superintendencia Financiera de Colombia ha establecido en la Circular Externa Básica Jurídica 029 de 2014 como en la Circular Externa Básica Contable 100 de 1995. En línea con lo anterior, FINDETER ha implementado los respectivos sistemas de administración de riesgos financieros, tales como, riesgo de liquidez, riesgo de mercado, riesgo de contraparte y riesgo de crédito; y los sistemas de administración de riesgos no financieros o riesgos operativos tales como, riesgo operativo, riesgos de seguridad de la información y ciberseguridad, riesgo de lavado de activos y financiación del terrorismo y riesgo de continuidad del negocio. Adicionalmente, como mejor práctica FINDETER ha implementado el respectivo sistema para la administración de riesgos ambientales y sociales.

En este marco, FINDETER implementa sus sistemas de riesgos financieros y no financieros de acuerdo con las disposiciones de dicha normatividad y los administra y gestiona según con las etapas allí especificadas, estableciendo políticas y metodologías para cada una de estas, las cuales se condensan en el manual de cada sistema, que son aprobados únicamente por la Junta Directiva.

Para ser más efectivo y eficiente en la administración de los riesgos operativos, FINDETER ha implemento un modelo integral para la gestión de este tipo de riesgos, el cual le permite la integración y administración de los siguientes sistemas de administración de riesgos operativos bajo una solo metodología: Sistema de Administración de Riesgo Operativo – SARO, Sistema de Administración del Riesgo de Lavado de Activos y financiación del Terrorismo – SARLAFT, Sistema de Administración de Riesgos de Seguridad de la Información y Ciberseguridad – SARSICIB y continuidad del negocio.

A continuación, se describen de forma general cada una de las metodologías propias para la administración del sistema de administración integral de riesgos operativo, que incluye también los riesgos de seguridad de la información, la cual se desarrolla a través de los procedimientos, instructivos, herramientas tecnológicas y demás mecanismos que se estimen pertinentes para su aplicación.

El modelo a través del cual se desarrolla la implementación del sistema de administración de riesgos operativo dentro de la entidad se presenta a continuación:

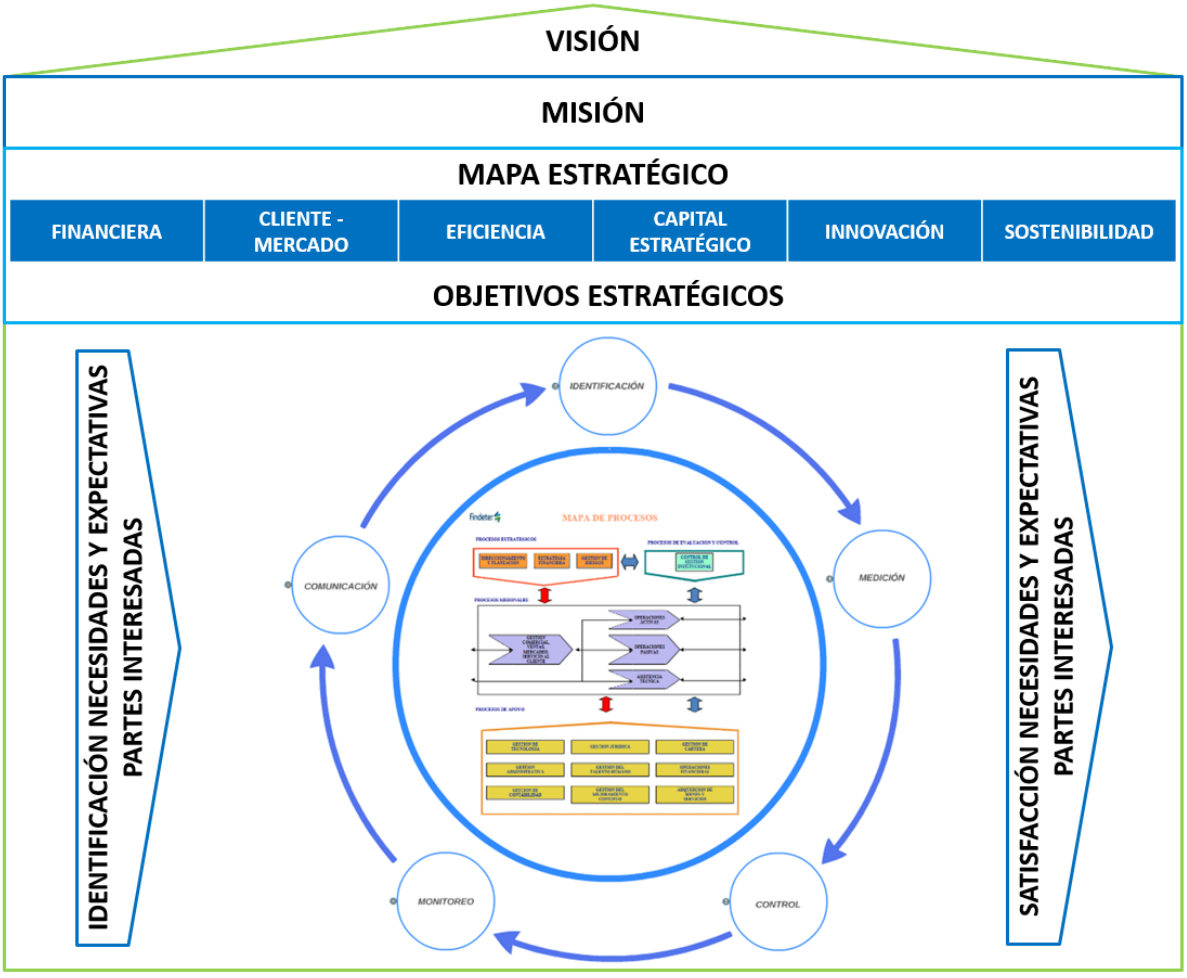

Figura 1. **Metodologías para la administración del riesgo operativo**
Fuente: Manual SARO de Findeter

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.

La identificación de los riesgos operativos, 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 URO. Teniendo en cuenta lo anterior, la gestión de los riesgos operativos 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.

5. ETAPAS PARA LA GESTION DE RIESGOS OPERATIVOS

Para la gestión del riesgo en FINDETER se establecen las siguientes etapas:

5.1. ETAPA DE IDENTIFICACION

FINDETER realiza la identificación de sus riesgos con un enfoque basado en procesos, donde toma como fundamento el objetivo de este para la definición de los riesgos. En esta etapa se considera el activo de información asociado al riesgo y proceso y se definen los factores teniendo en cuenta las directrices de la norma y los definidos en el Comité de Basilea.

La identificación del riesgo es responsabilidad de la primera línea de defensa, es decir del dueño del proceso, el cual cuenta con la asesoría permanente de la segunda línea de defensa, la Vicepresidencia de Riesgos.

En esta etapa se define el riesgo, sus causas, fuentes, procesos y activos de información asociados, así como el responsable de su gestión.

5.2. ETAPA DE MEDICION

La Vicepresidencia de Riesgos de la entidad establece las métricas para la medición de la probabilidad e impacto de los riesgos identificados por el Líder de Proceso. Esta metodología se basa en una medición de una matriz de cinco (5) por cinco (5) con los siguientes rangos:

PROBABILIDAD	
Nro.	NIVEL
1	Raro
2	Improbable
3	Posible
4	Probable
5	Certeza

IMPACTO	
Nro.	NIVEL
1	Insignificante
2	Menor
3	Moderado
4	Mayor
5	Catastrófico

Figura 2. **Métricas para medición de probabilidad e impacto**
Fuente: Manual SARO de la entidad

En esta etapa se establecen el impacto económico basado en el patrimonio técnico de FINDETER, el impacto legal, reputacional y operativo el cual incluye los aspectos asociados a la seguridad de la información (disponibilidad, integridad y confidencialidad), los cuales se consideran relevantes para la continuidad del negocio y, finalmente el impacto asociado al contagio que se deriva de riesgos asociados a lavado de activos y financiación del terrorismo

Como resultado de lo anterior es posible establecer la severidad del riesgo y ubicarlo en el mapa de riesgos. Esto permite al Líder del Proceso priorizar los riesgos sobre los cuales se debe tener mayor control.

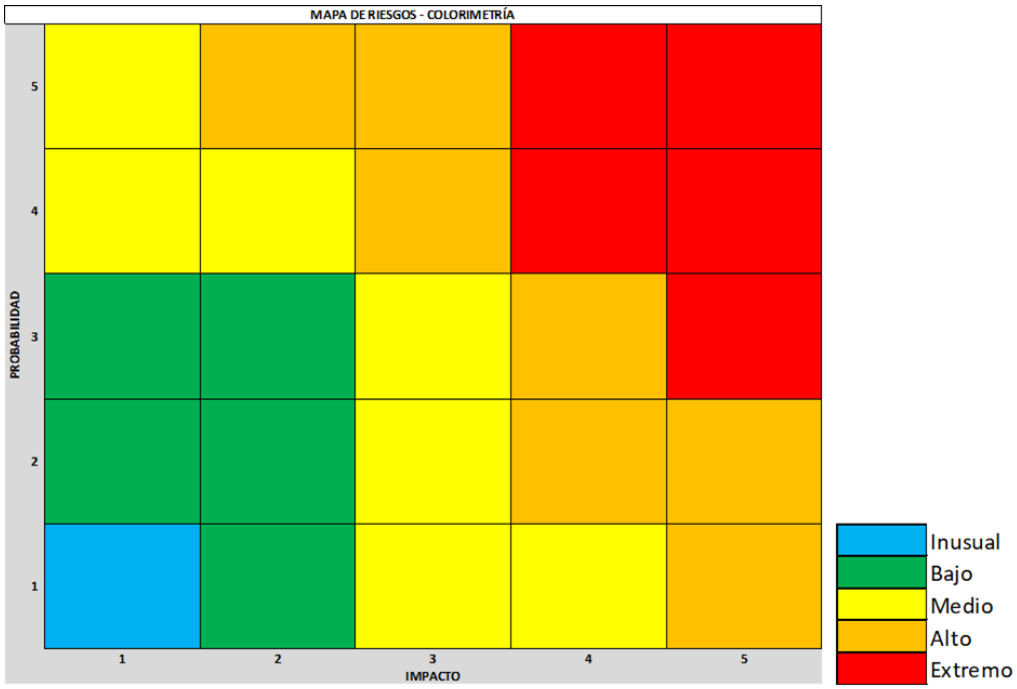

Figura 3. **Mapa de Riesgos**
Fuente: Manual SARO de la entidad

5.3. ETAPA DE CONTROL

Esta etapa para la gestión de los riesgos operativos es responsabilidad del Líder del Proceso, ya que debe definir las acciones concretas a través de las cuales gestionará el riesgo y/o custodiará los activos a su cargo.

La Vicepresidencia de Riesgos define una metodología que permite establecer la efectividad de los controles, definiendo en qué proporción se disminuye el riesgo.

Los controles deben estar documentados preferiblemente dentro de los procedimientos del Sistema Integrado de Gestión de FINDETER con el objeto de contar con la trazabilidad necesaria de su aplicación, así como la exigibilidad de su uso por parte de los encargados de su ejecución.

5.4. ETAPA DE MONITOREO

FINDETER cuenta con diversas herramientas de monitoreo de los riesgos a cargo de las tres líneas de defensa. En cuanto a la primera línea de defensa o Líder de Proceso, debe supervisar que los controles de su proceso se estén ejecutando a través de la definición de indicadores de gestión, revisiones aleatorias u otros mecanismos que considere

pertinentes. Así mimo, debe registrar los eventos de riesgo materializados (incidentes de seguridad), en cumplimiento de la norma de la SFC.

La segunda línea de defensa, es decir la Vicepresidencia de Riesgos, realiza pruebas de recorrido a los controles para asegurar su funcionamiento, monitorea el perfil de riesgo, analiza los eventos registrados y apoya a los Líderes de Proceso en la definición de los planes de acción para asegurar que no se vuelvan a materializar. Es importante resaltar que la Vicepresidencia de Riesgos tiene acceso a la información de FINDETER que sea que requiera para asesorar adecuadamente a la primera línea de defensa en la gestión de sus riesgos.

La auditoría tanto interna como externa o tercera línea de defensa, de acuerdo con la normatividad aplicable, adelanta periódicamente las auditorías necesarias, cuyos resultados son insumo para que el Líder del Proceso fortalezca la gestión de los riesgos.

6. ESQUEMA MODELO DE SEGURIDAD ALINADO A RIESGOS

7. 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 vigilancia y control y el Gobierno Nacional.

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:

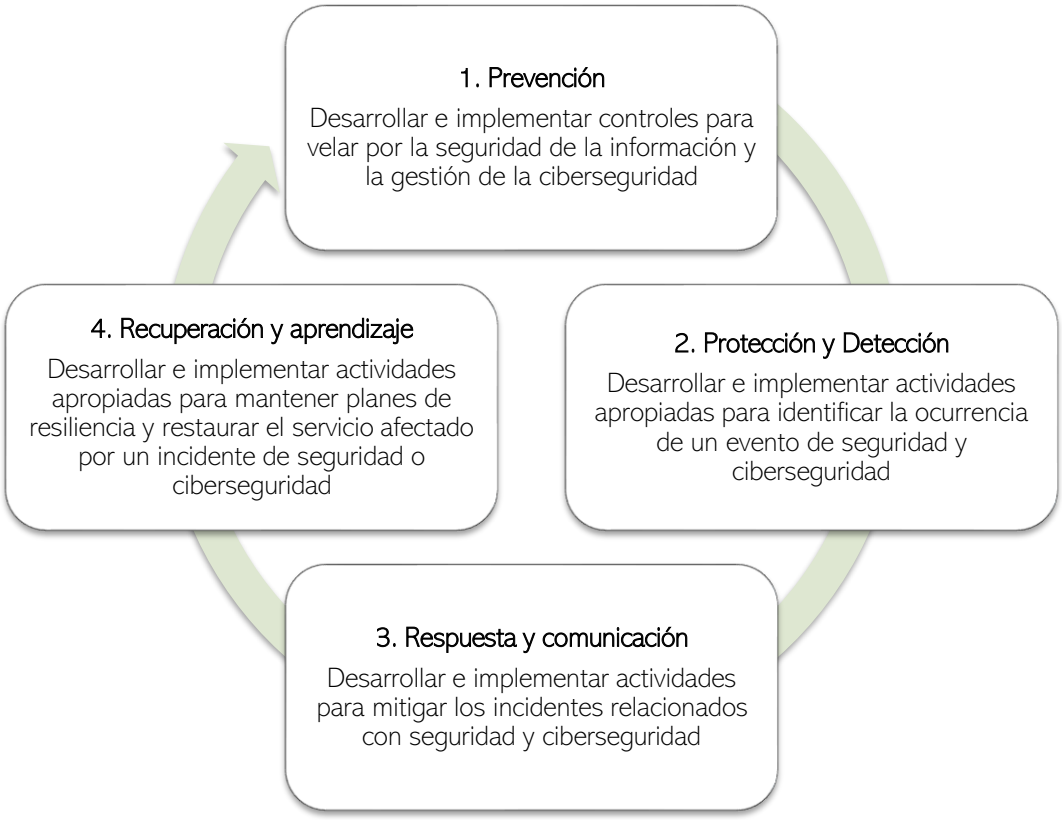

Figura 4. **Fase Implementación CE007/2018 SFC**

La implementación de los requerimientos establecido en la CE007/2018 de la SFC le ha permitido a FINDETER fortalecer la gestión de los riesgos de seguridad de la información, seguridad digital y ciberseguridad en los siguientes aspectos:

- Actualización de las políticas y procedimientos para gestionar efectivamente el riesgo de ciberseguridad.
- Establecimiento y formalización de la unidad que gestiona los riesgos de seguridad de la información y la ciberseguridad en FINDETER.
- Actualización de la metodología integral de riesgos operativos de FINDETER con el objetivo de: (i) alinear la gestión de riesgos de ciberseguridad, (ii) incluir otras fuentes de información que permitan identificar situaciones que afecten o puedan afectar la seguridad de FINDETER, (iii) formalizar las funciones de la Unidad de Gestión de Riesgos de Seguridad de la Información y Ciberseguridad e (iv) incluir la identificación y valoración de activos y ciber-activos de información.

- Identificación, administración y tratamiento de los riesgos cibernéticos emergentes que puedan llegar a afectar a FINDETER.
- Ampliación de las fuentes de información para la la identificación de riesgos de seguridad de la información y ciberseguridad, tales como: (i) Monitoreo, análisis y correlación sobre los eventos de seguridad que generen los dispositivos de la Entidad, (ii) Monitoreo permanente sobre las amenazas internas, externas y del ciberespacio que puedan afectar la seguridad de la información de la Entidad y (iii) Monitoreo de diferentes fuentes de información en el ciberespacio correspondientes a redes indexadas tales como sitios web, blogs y redes sociales, o redes no indexadas, con el propósito de identificar posibles ataques cibernéticos contra FINDETER.
- Fortalecimiento de la gestión de eventos y vulnerabilidades de seguridad de la información y ciberseguridad.
- Fortalecimiento en los contratos que se celebran con terceros críticos, de medidas y obligaciones pertinentes para la adopción y el cumplimiento de políticas para la gestión de los riesgos de seguridad de la información y ciberseguridad.
- Colaboración e intercambio de información con las autoridades que hacen parte del modelo nacional de gestión de incidentes cibernéticos y la atención oportuna de los boletines de seguridad emitidos por estos organismos.

8. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACION Y CIBERSEGURIDAD 2020

Actividad	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Set	Oct	Nov	Dic
Identificación de riesgos. Tarea permanente que se realiza según lo dispuesto en la metodología integral de riesgos de la entidad												
Medición de riesgos. Tarea permanente que se realiza según la metodología integral de riesgos de la entidad para establecer el perfil de riesgos inherente.												
Control de riesgos. Tarea permanente que se realiza según la metodología integral de riesgos de la entidad para establecer el perfil de riesgo residual.												
Monitoreo de riesgos. Tarea permanente que se realiza según la metodología integral de riesgos de la entidad para establecer la efectividad de los controles establecidos e informar a la alta dirección y a la junta directiva sobre su desempeño.												
Elaborar primer informe de desempeño y gestión del sistema SARSICIB												
Presentar primer informe de gestión del sistema SARSICIB a la Junta Directiva y al comité de auditoria												
Elaborar segundo informe de desempeño y gestión del sistema SARSICIB												
Presentar segundo informe de gestión del sistema SARSICIB a la Junta Directiva y al comité de auditoria												
Ejecutar análisis de vulnerabilidades primer ciclo												
Mitigar vulnerabilidades del primer ciclo												
Ejecutar análisis de vulnerabilidades segundo ciclo												
Mitigar vulnerabilidades del segundo ciclo												
Ejecutar la prueba anual de Hacking Ético												

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.

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.

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.