



FINDETER

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION Y CIBERSEGURIDAD 2021

SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION
SISTEMA DE ADMINISTRACION DE RIESGOS DE SEGURIDAD DE LA INFORMACION Y CIBERSEGURIDAD - **SARSICIB**
VICEPRESIDENCIA DE RIEGOS
FINDETER
2021



Contenido

1.	INTRODUCCION.....	3
2.	OBJETIVOS	5
2.1.	OBJETIVO GENERAL.....	5
2.2.	OBJETIVO ESPECIFICOS.....	5
3.	METODOLOGIA ESTABLECIMIENTO MODELO DE SEGURIDAD	6
3.1.	CICLO OPERACIÓN	6
3.2.	ALINEACION NORMA ISO 27001:2013 VS CICLO DE OPERACION	7
3.3.	FASES I: DIAGNOSTICO.....	9
3.4.	FASES II: PLANIFICACION	10
3.5.	FASES III: IMPLEMENTACION.....	14
3.6.	FASES IV: EVALUACION DE DESEMPEÑO	16
3.7.	FASES V: MEJORA CONTINUA.....	17
4.	MEJORA CONTINUA MODELO DE SEGURIDAD DE FINDETER	18
5.	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2021	20
6.	TERMINOS Y REFERENCIAS	22



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 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 Información y Ciberseguridad denominado SARSICIB para la debida administración y gestión de las situaciones 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 relacionadas con seguridad de la información dadas por el Gobierno Nacional y la Superintendencia Financiera de Colombia – SFC, tales como:

- Circular Básica Jurídica (CE029/14) 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 del riesgo de 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).
- Directiva Presidencial 03 de marzo 15 de 2021, que se establece lineamientos para el Uso de Servicios en la Nube, Seguridad Digital y Gestión de Datos.
- Resolución No. 00500 de marzo 10 de 2021, que 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.
- Política Nacional de Seguridad Digital.



- Ley 1581 de 2012 y sus decretos reglamentarios - Protección de Datos personales.
- Ley 1712 de 2014 y sus decretos reglamentarios - Transparencia y derecho de acceso a la información pública nacional.
- Entre otras.

El presente documento contiene el plan de seguridad de la información 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. OBJETIVOS

2.1. OBJETIVO GENERAL

Establecer un plan de seguridad de la información y de ciberseguridad para el año 2021 que apoye 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 2021 que apalancan el cumplimiento del objetivo general:

- OE1. Apoyar la operación, mejora continua y sostenibilidad del SGSI y SARSICIB de FINDETER.
- OE2. Fortalecer y optimizar la gestión de la seguridad de la información, seguridad digital y ciberseguridad al interior de FINDETER.
- 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.
- OE4. Fortalecer la cultura de seguridad de la información y ciberseguridad en FINDETER.
- OE5. Atender las observaciones, recomendaciones hallazgos de las auditorías internas y externas de control y vigilancia.
- OE6. Atender los requerimientos de seguridad de la información, seguridad digital y ciberseguridad establecidos por el Gobierno Nacional y la SFC.

3. METODOLOGIA ESTABLECIMIENTO MODELO DE SEGURIDAD

3.1. 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:

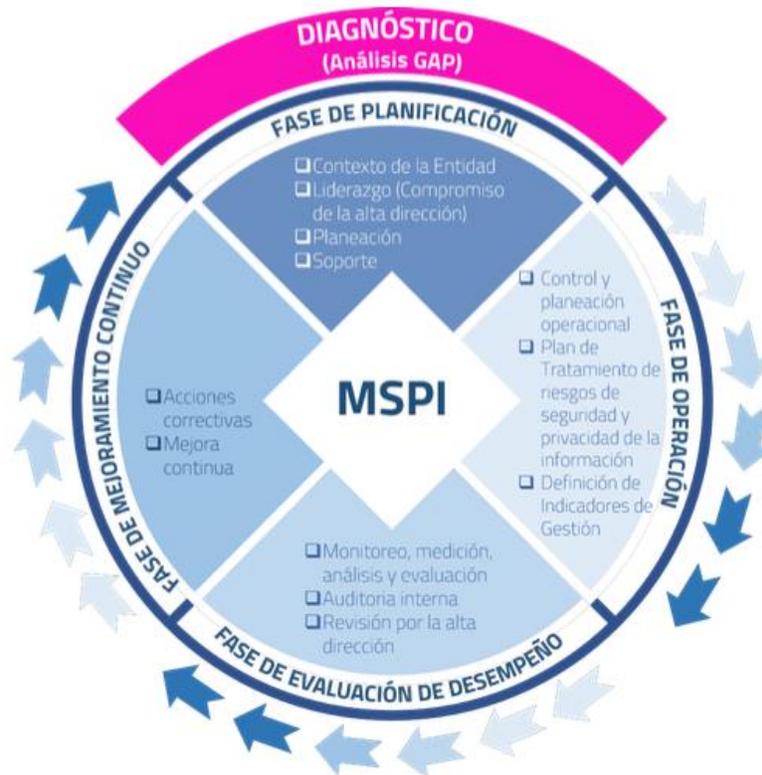


Figura 1. **Ciclo del Modelo de Seguridad y Privacidad de la Información**

Fuente: Documento Maestro del Modelo de Seguridad y Privacidad de la Información Versión 4.0
Ministerio de Tecnologías de la Información y las Comunicaciones

- **Fase Diagnóstico:** Permite identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información
- **Fase Planificación (Planear):** 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.

¹ Modelo de Seguridad y Privacidad, MINTIC, Pág. 1-2



- **Fase Implementación (Hacer):** En esta fase se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas.
- **Fase Evaluación de desempeño (Verificar):** Una vez implantada la mejora, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas.
- **Fase Mejora Continua (Actuar):** 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.

3.2. 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:

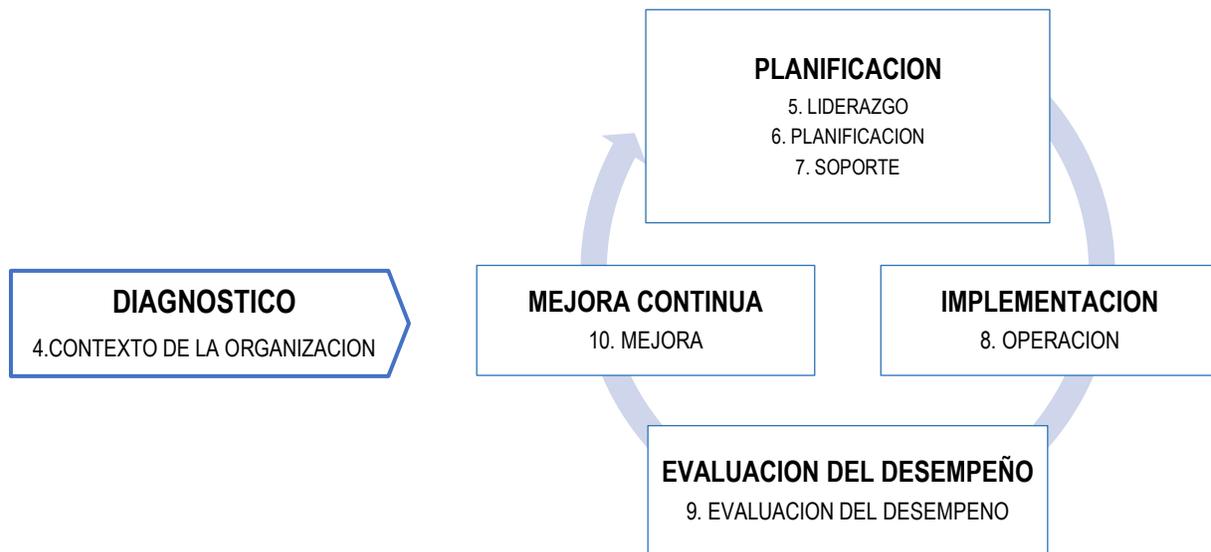


Figura 2. Norma ISO 27001:2013 alineado al Ciclo de mejora continua

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	Capítulo 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 cuestiones externas e internas de la organización y de su contexto, con el propósito de incluir las necesidades y expectativas de las partes interesadas 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 controlar los procesos necesarios para cumplir los objetivos y requisitos

² NTC-ISO-IEC 27001:2013, Pág. 1-12



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.

3.3. 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	Diagnóstico de la situación actual de la entidad con relación a la gestión de seguridad de la información.



privacidad de la información al interior de la Entidad	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 ' <i>ANEXO 3: ESTRATIFICACIÓN DE ENTIDADES</i> ' 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 ' <i>MODELO DE MADUREZ</i> ' 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 la 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.

3.4. 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.

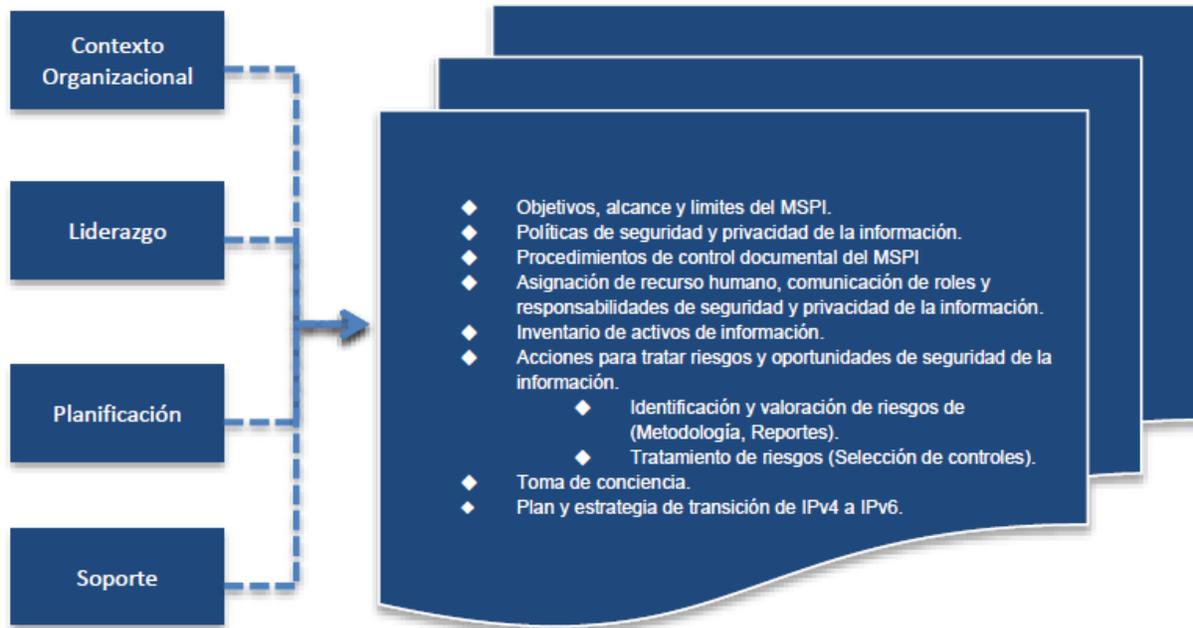


Figura 4. Fase de planificación modelo de seguridad

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.
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. 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.



	<p>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.</p> <p>Definir la estructura organizacional de la Entidad que contendrá los roles y responsabilidad pertinentes a la seguridad de la información.</p>
Definir la metodología de riesgos de seguridad de la información	<p>Definir Metodología de Valoración de Riesgos de Seguridad.</p> <p>Integrar la metodología definida con la metodología de riesgos operativos de la entidad.</p> <p>Implementar un sistema de información para la administración y gestión de los riesgos de seguridad de la entidad.</p>
Elaborar las políticas de seguridad y privacidad de la información de la entidad	<p>Elaborar Política General de Seguridad y Privacidad la cual debe ser aprobada por la Alta Dirección y socializada al interior de la Entidad.</p> <p>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.</p>
Elaborar documentación de operación (formatos de procesos, procedimientos y documentos debidamente definidos y establecidos) del sistema de seguridad de la información	<p>Elaborar los documentos de operación del sistema de seguridad de la información, tales como:</p> <ul style="list-style-type: none">• Declaración de aplicabilidad• Procedimiento y/o guía de identificación y clasificación de activos de información.• Procedimiento Continuidad del Negocio, Procedimientos operativos para gestión de TI• Procedimiento para control de documentos (SGI)• Procedimiento para auditoría interna (SGI)• Procedimiento para medidas correctivas (SGI)• Procedimiento para la gestión de eventos e incidentes de seguridad de la información• Procedimiento para la gestión de vulnerabilidades de seguridad de la información.• Entre otros.
Identificar y valorar activos de información	<p>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.</p> <p>Documentar el inventario de los activos de información de la entidad.</p>



<p>Identificar, valorar y tratar los riesgos de seguridad de la información de la entidad</p>	<p>Realizar la identificación y valoración de los riesgos transversales de seguridad de la información y definir los respectivos planes de tratamiento.</p> <p>Realizar la valoración de riesgos de seguridad de la información y ciberseguridad.</p> <p>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 selección 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.</p>
<p>Establecer plan de capacitación, comunicación y sensibilización de seguridad de la información.</p>	<p>Elaborar plan anual de capacitación y sensibilización anual de seguridad de la información y ciberseguridad.</p>
<p>Establecer Plan de diagnóstico de IPv4 a IPv6</p>	<p>Realizar el diagnóstico para la transición de la entidad de IPv4 a IPv6.</p> <p>Documentar el Plan de diagnóstico para la transición de IPv4 a IPv6.</p>

3.5. 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 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 Ingeniería Social	Ejecutar pruebas anuales de ingeniería social orientadas a verificar aspectos como: (i) los protocolos internos de seguridad, (ii) el nivel de concientización de los funcionarios y terceros que laboren en la entidad sobre temas de seguridad de la información, (iii) el conocimiento y/o cumplimiento de las políticas de seguridad y privacidad de la información de la entidad y (iv) el nivel de exposición de la información publicada en internet de la entidad y de sus empleados.

3.6. 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 auditoría 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.



3.7. 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.



4. 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:

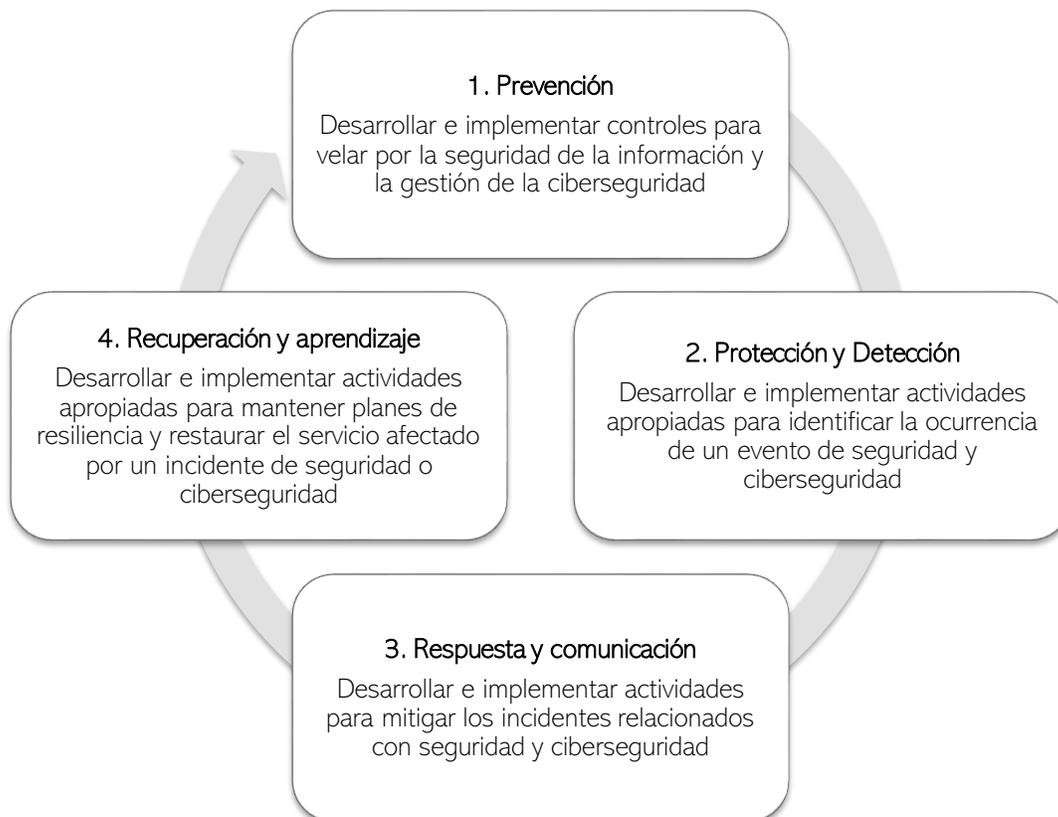


Figura 8. Fase Implementación CE007/2018 SFC



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 establecidos a 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.



5. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2021

Dependencia	Nombre de la tarea	Descripción	Política de Gestión y Desempeño	Fecha Inicio	Fecha Fin	Fuente de Financiación
Vicepresidencia de Riesgos	Sensibilización y socialización temas de seguridad de la información y ciberseguridad al interior de la entidad	Realizar actividades y/o publicar de forma periodica temas relacionados con seguridad de la información y/o ciberseguridad con el objetivo de fortalecer la cultura de seguridad en la entidad	Seguridad Digital	1/01/2021	31/12/2021	Findeter
Vicepresidencia de Riesgos	Ejecución campañas seguridad de la información y ciberseguridad para clientes externos	Realizar de campañas de seguridad seguridad de la información y/o ciberseguridad para clientes externo	Seguridad Digital	1/01/2021	30/06/2021	Findeter
Vicepresidencia de Riesgos	Análisis GAP ISO 27001	Realizar un análisis GAP del nivel de cumplimiento de la norma ISO 27001 e identificar las brechas de cumplimiento	Seguridad Digital	1/01/2021	30/03/2021	Findeter
Vicepresidencia de Riesgos	Contratar servicios de seguridad gestionada soportados en un SOC	Realizar el proceso de contratación de los servicios de seguridad gestionada soportados en un SOC	Seguridad Digital	1/03/2021	30/06/2021	Findeter
Vicepresidencia de Riesgos	Fortalecer monitoreo de amenazas	Fortalecer el monitoreo y correlación de eventos de seguridad de la información y ciberamenazas	Seguridad Digital	1/01/2021	31/12/2021	Findeter
Vicepresidencia de Riesgos	Fortalecer gestión de incidentes de seguridad de la información	Fortalecer el proceso de identificación y gestión de los incidentes de seguridad de la información y alineación con los eventos de riesgos	Seguridad Digital	1/01/2021	30/04/2021	Findeter
Vicepresidencia de Riesgos	Cumplimiento circular 033 de 2020 SFC	Dar cumplimiento a los requerimientos establecidos por la SFC en la CE 033 de 2020	Seguridad Digital	1/01/2021	30/04/2021	Findeter
Vicepresidencia de Riesgos	Ejecución análisis de vulnerabilidades primera prueba anual (Q1)	Ejecutar la primera prueba anual de analisis vulnerabilidades sobre la infraestructura tecnologica de la entidad	Seguridad Digital	15/01/2021	30/03/2021	Findeter



Dirección de Tecnología	Mitigación de vulnerabilidades primera prueba (Q1)	Mitigar las vulnerabilidades identificadas en la primera prueba de vulnerabilidades	Seguridad Digital	1/04/2021	30/06/2021	Findeter
Vicepresidencia de Riesgos	Ejecución análisis de vulnerabilidades primera prueba anual (Q2)	Ejecutar la segundo prueba anual de analisis vulnerabilidades sobre la infraestructura tecnologica de la entidad	Seguridad Digital	1/07/2021	30/09/2021	Findeter
Dirección de Tecnología	Mitigación de vulnerabilidades primera prueba (Q2)	Mitigar las vulnerabilidades identificadas en la segunda prueba de vulnerabilidades	Seguridad Digital	1/10/2021	31/12/2021	Findeter
Dirección de Tecnología	Mitigación resultados prueba de Hacking Etico 2020	Mitigar las vulnerabiidades y/o debilidades de seguridad encontradas en la prueba de Hacking Etico realizada en el cuarto trimestre de 2020	Seguridad Digital	1/01/2021	30/06/2021	Findeter
Vicepresidencia de Riesgos	Ejecución Prueba de Hacking Etico	Ejecutar la prueba anual de Hacking Etico	Seguridad Digital	1/07/2021	31/12/2021	Findeter
Vicepresidencia de Riesgos	Ejecución Prueba de Ingenieria Social	Ejecutar prueba anual de ingenieria social	Seguridad Digital	1/07/2021	31/12/2021	Findeter



6. 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.

Ciberriesgo o 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 se caracteriza por ausencia en controles de seguridad que permite ser explotada.