SuperSubsidio
Vigilamos tu caja de compensación

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2023

Sede Principal: Edificio World Business Port
Cra 69 # 25B - 44 Pisos 3, 4 y 7
Teléfonos: (601) 3487777 - PBX: (601) 3487800
Fax: (601) 3487804
https://www.ssf.gov.co - E-mail: ssf@ssf.gov.co
Bogotá D.C., Colombia

Control del Documento

Nivel de Seguridad	*Confidencial, Uso Interno*			
Entidad	Superintendencia de Subsidio Familiar			
Área	Oficina de Tecnologías de la Información y las Comunicaciones			
Revisado por	Oficina de Tecnologías de la Información y las Comunicaciones		**Fecha (dd-mm-aa)**	13/01/2023
Versión	**Fecha (dd-mm-aa)**	**Descripción del Cambio**	**Comentarios**	**Por**
1.0	13/01/2023	Primera versión del documento		Luisa Fernanda Pardo Sánchez

1. OBJETIVO

Definir la planificación de las actividades orientadas a gestionar y fortalecer el tratamiento de los riesgos asociados a la seguridad y privacidad de la información, que es generada, tratada y custodiada por la Superintendencia de Subsidio Familiar de ahora en adelante denominada SSF en el presente documento; con el fin preservar la confidencialidad, integridad y disponibilidad, de la información en la entidad.

1.1 OBJETIVOS ESPECÍFICOS

- Fortalecer el Sistema de Gestión de Seguridad y Privacidad de la Información de la SSF, mediante la implementación y mejora de los controles de seguridad alineados con el Modelo de seguridad y privacidad de la información y la ISO 27001:2013.
- Gestionar los riesgos de seguridad y privacidad de la información de la entidad alineado con los requerimientos metodológicos de la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP.
- Apoyar la evaluación y revisión de los controles definidos en el plan de tratamiento de los riesgos de seguridad de la información.

2. DEFINICIONES

- **Activo de información**: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma, el cual tiene valor para la SSF por lo tanto para ello se tienen contemplados los siguientes activos de información: personas, información/dato, hardware, software, redes, infraestructura y servicios.
- **Control**: Son las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Seguridad de la información**: Conjunto de medidas que toman las personas y las organizaciones, que les permiten resguardar y proteger los activos de información, preservando su Confidencialidad, Integridad y Disponibilidad.
- **Confidencialidad:** Propiedad que impide la divulgación de información a personas o sistemas no autorizados.
- **Disponibilidad:** Característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.
- **Integridad:** Garantía de la exactitud y completitud de la información de la información y los métodos de su procesamiento.
- **Sistema de Gestión de Seguridad y Privacidad de la Información**: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

3. MARCO LEGAL

Dentro del marco legal más relevante para justificar el presente plan de seguridad y privacidad de la información y Tratamiento de Riesgos, se encuentran las siguientes normas:

- **Ley 1437 de 2011, Capítulo IV**, “utilización de medios electrónicos en el procedimiento administrativo”. “Los procedimientos y trámites administrativos podrán realizarse a través de medios electrónicos. Para garantizar la igualdad de acceso a la administración, la autoridad

deberá asegurar mecanismos suficientes y adecuados de acceso gratuito a los medios electrónicos, o permitir el uso alternativo de otros procedimientos."

- **Ley 1581 de 2012**, g) Principio de seguridad: "La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento". Artículo 17, ítem d: "Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento".
- **Ley 1712 de 2014**, "principio de transparencia": "Principio conforme al cual toda la información en poder de los sujetos obligados definidos en esta ley se presume pública, en consecuencia de lo cual dichos sujetos están en el deber de proporcionar y facilitar el acceso a la misma en los términos más amplios posibles y a través de los medios y procedimientos que al efecto establezca la ley, excluyendo solo aquello que esté sujeto a las excepciones constitucionales y legales y bajo el cumplimiento de los requisitos establecidos en esta ley".
  Artículo 7: "Disponibilidad de la información" "En virtud de los principios señalados, deberá estar a disposición del público la información a la que hace referencia la presente ley, a través de medios físicos, remotos o locales de comunicación electrónica. Los sujetos obligados deberán tener a disposición de las personas interesadas dicha información en la web, a fin de que estas puedan obtener la información, de manera directa o mediante impresiones. Asimismo, estos deberán proporcionar apoyo a los usuarios que lo requieran y proveer todo tipo de asistencia respecto de los trámites y servicios que presten."
  Título III "Excepciones acceso a la información" "Información exceptuada por daño de derechos a personas naturales o jurídicas. Es toda aquella información pública clasificada, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito."
- **Conpes 3854 de 2016**, objetivo general "Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país".
- **Decreto 1413 de 2007**, artículo 2.2.17.6.5, "Privacidad por diseño y por defecto": "Los operadores de servicios ciudadanos digitales deberán atender las buenas prácticas y principios desarrollados en el ámbito internacional en relación con la protección y tratamiento de datos personales que son adicionales a la Accountability, y que se refieren al Privacy by design (PbD) y Privacy Impact Assessment (PIA), cuyo objetivo se dirige a que la protección de la privacidad y de los datos no puede ser asegurada únicamente a través del cumplimiento de la normativa, sino que debe ser un 'modo de operar de las organizaciones, y aplicarlo a los sistemas de información, modelos, prácticas de negocio, diseño físico, infraestructura e interoperabilidad, que permita garantizar la privacidad al ciudadano y a las empresas en relación con la recolección, uso, almacenamiento, divulgación y disposición de los mensajes de datos para los servicios ciudadanos digitales gestionados por el operador".
- **Decreto 1008 de 2018** "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones". **ARTÍCULO 2.2.9.1.1.3.** Principios. "Seguridad de la Información: Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano".
- **Decreto 612 de 2018**, artículo 1. "Integración de planes institucionales y estratégico. Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web."

- **Resolución 500 de 2021,** El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) expide la Resolución 500 de 2021, "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".
- **Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 - Diciembre de 2020,** 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. En esta versión 5 se actualizaron y precisaron algunos elementos metodológicos para mejorar el ejercicio de identificación y valoración del riesgo.

4. GENERALIDADES

El presente plan de tratamiento de riesgos está orientado a mejorar por medio de la implementación acciones concretas la gestión de los riesgos de seguridad y privacidad de la Información de la SSF; para tal fin es necesario mencionar que estas acciones están enmarcadas a intervenir los 3 componentes del modelo (Personas, Procesos y Tecnología). Para la ejecución del presente Plan es necesario definir los siguientes acuerdos entre las partes interesadas:

- **Compromiso:** Para la ejecución del plan es necesaria la participación de los diferentes niveles de decisión de la SSF (estratégico, táctico y operativo), especialmente para la valoración de procesos frente a las normas ISO 27001/2:2013, así como también se asume el compromiso y el involucramiento de todos los Stackeholders de la Entidad.
- **Población Objetivo:** Para asegurar el éxito en la ejecución del plan es prioritario involucrar a las personas que ejercen responsabilidades de seguridad de la información en la SSF las cuales están identificadas en la matriz de roles y responsabilidades del Sistema de Gestión de Seguridad y Privacidad de la Información; así como también todos aquellos colaboradores que deben apoyar y/o asistir a las reuniones y entrevistas que se llevaran a cabo para el levantamiento de la información requerida y que por su actuar están directa o indirectamente relacionados con los procesos y procedimientos establecidos en el SGSI.
- **Duración:** El tiempo estimado para la ejecución del plan es de 11 meses contados a partir de la aprobación del presente plan de trabajo.
- **Seguimiento:** Se establece un seguimiento trimestral a la ejecución de las actividades propuestas en el plan.

5. PLANIFICACIÓN DE ACTIVIDADES

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la SuperSubsidio Familiar 2023				
Categoría	**Actividad**	**Responsable**	**F Inicial**	**F Final**
Definición y seguimiento del plan de tratamiento de riesgos de seguridad y privacidad de la información 2023	Definición del Plan de tratamiento de Riesgos de seguridad, privacidad de la información	Equipo de seguridad	1/1/2023	30/01/2023
Actualización del perfil de riesgos de Seguridad digital y protección de datos personales	Actualización del perfil de riesgos de seguridad y privacidad de la información	Equipo de seguridad	1/06/2023	30/09/2023
	Revisión y actualización del plan de tratamiento de riesgos de seguridad, privacidad de la	Equipo de seguridad	1/10/2023	30/11/2023

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la SuperSubsidio Familiar 2023				
Categoría	**Actividad**	**Responsable**	**F Inicial**	**F Final**
	información y protección de datos personales en la entidad			
Implementación del plan de tratamiento de riesgos de seguridad digital de la SSF	Evaluar los controles definidos en el plan de tratamiento de riesgos de seguridad digital.	Equipo de seguridad	3/03/2023	15/12/2023
	Revisión y pruebas del plan de copias de respaldo I semestre	Equipo de seguridad	3/03/2023	15/06/2023
	Revisión y pruebas del plan de copias de respaldo II semestre	Equipo de seguridad	3/07/2023	15/12/2023
	Realizar seguimiento al plan de mantenimiento de infraestructura TIC y equipos de cómputo para la vigencia 2023 I semestre	Equipo de seguridad	3/03/2023	15/07/2023
	Realizar seguimiento al plan de mantenimiento de infraestructura TIC y equipos de cómputo para la vigencia 2023 II semestre	Equipo de seguridad	1/07/2023	30/12/2023
	Revisión y depuración periódica de usuarios a los sistemas de información I semestre 2023	Equipo de seguridad	3/03/2023	15/07/2023
	Revisión y depuración periódica de usuarios a los sistemas de información II semestre 2023	Equipo de seguridad	1/07/2023	30/12/2023
	Realizar el análisis de vulnerabilidades a los sistemas de información de la entidad	Equipo de seguridad	3/03/2023	15/12/2023