Supersubsidio

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

SuperSubsidio
Dirección: Carrera 69 No. 25B - 44. Pisos 3, 4 y 7
Edificio World Business Port
Conmutador: (+57) (601) 348 78 00
Línea Gratuita: (+57) 018000 910 110
Correo institucional: ssf@ssf.gov.co

1. INTRODUCCIÓN

El Plan de Seguridad de la Información de la entidad tiene como propósito establecer el marco estratégico, operativo y tecnológico que permite proteger los activos de información, garantizar la prestación continua de los servicios institucionales y asegurar la confianza de la ciudadanía en la gestión pública.

En un entorno cada vez más digital, las entidades del Estado se enfrentan a amenazas crecientes que pueden comprometer la confidencialidad, integridad, disponibilidad y privacidad de la información, así como la continuidad de los procesos misionales. Estas amenazas incluyen incidentes cibernéticos, fallas tecnológicas, errores humanos, uso inadecuado de los sistemas de información y eventos externos que pueden afectar la operación institucional.

Este plan se fundamenta en los principios del Gobierno Digital, las directrices del Modelo Integrado de Planeación y Gestión (MIPG), el cumplimiento del Marco de Seguridad y Privacidad de la Información, y las mejores prácticas recogidas en estándares internacionales como ISO/IEC 27001, ISO 27002, ISO 22301, ISO 27005 e ISO 27035.

El documento define los lineamientos, políticas, roles, responsabilidades, controles, procedimientos y estrategias necesarios para gestionar los riesgos de seguridad de la información, responder oportunamente ante incidentes, fortalecer la continuidad del negocio y garantizar la protección de datos personales tratados por la entidad.

Finalmente, este plan busca promover una cultura institucional de seguridad, asegurar una administración eficaz de los recursos tecnológicos y garantizar que la entidad cumpla con sus obligaciones legales, normativas y misionales, contribuyendo al fortalecimiento de la transparencia, la confianza pública y la prestación eficiente de los servicios a la ciudadanía.

2. OBJETIVO

Establecer el marco estratégico, organizacional y operativo que permita proteger los activos de información de la entidad, garantizando su confidencialidad, integridad, disponibilidad y privacidad, mediante la implementación de políticas, controles, procedimientos y mecanismos de gestión de riesgos que aseguren la continuidad de los servicios institucionales, el cumplimiento normativo y la confianza de la ciudadanía en la administración pública.

3. OBJETIVOS ESPECIFICOS

- Establecer una estructura de gobierno de seguridad de la información que defina roles, responsabilidades y mecanismos de coordinación para garantizar la gestión integral de la seguridad en toda la entidad.
- Identificar, analizar y gestionar los riesgos de seguridad de la información, implementando controles y medidas de mitigación que reduzcan la probabilidad e impacto de incidentes que puedan afectar los procesos misionales.

- Implementar y mantener políticas, estándares y procedimientos de seguridad, alineados con la normatividad nacional y los marcos internacionales reconocidos, que orienten el uso adecuado y seguro de la información y los recursos tecnológicos.

- Fortalecer la protección de los datos personales y la privacidad, garantizando el tratamiento adecuado conforme a las disposiciones de la Ley 1581 de 2012, sus decretos reglamentarios y las políticas institucionales.

- Establecer capacidades para la prevención, detección, respuesta y recuperación ante incidentes de seguridad, mediante el desarrollo de procesos y herramientas que aseguren una actuación oportuna y coordinada.

- Promover la continuidad del negocio y la recuperación de desastres, asegurando la disponibilidad de los procesos y servicios esenciales mediante la creación, mantenimiento y pruebas periódicas de planes y estrategias de continuidad.

- Fortalecer la cultura institucional de seguridad de la información, a través de programas de sensibilización, formación y divulgación para funcionarios, contratistas y terceros con acceso a la información de la entidad.

- Garantizar el cumplimiento de los requisitos legales, normativos y contractuales, así como el seguimiento continuo a su implementación y mejora, a través de mecanismos de auditoría, evaluación y revisión periódica.

- Monitorear y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI) mediante indicadores, evaluaciones internas y acciones correctivas que aseguren su eficacia y pertinencia.

4. ALCANCE

El presente documento aplica a todo el modelo de operación por procesos de la Superintendencia de Subsidio Familiar, dando cumplimiento a lo establecido en el Decreto 1083 de 2015, “por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública”, al Capítulo 1 del Título 9 del Decreto 1078 de 2015, “por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”, así como el Modelo de Seguridad y Privacidad de la Información de la Resolución 500 de 2021 y la actualización del Anexo 1 en la resolución 02277 de 2025, alineado con la NTC/IEC ISO 27001.

5. DOCUMENTOS DE REFERENCIA

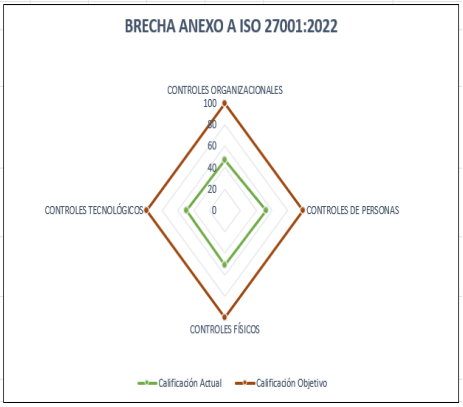
El Plan Estratégico de Seguridad de la Información se basa en los siguientes documentos, normas y lineamientos para su estructura y funcionamiento:
Constitución, leyes y directivas

- Artículos 15, 20, 23 y 74 de la Constitución Política de Colombia, referente al derecho al habeas data, el derecho a la intimidad, el derecho a la información, derecho de petición y derecho de acceso a la información pública.
- Ley 23 de 1982, "sobre derechos de autor".
- Ley 44 de 1993, "por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944".
- Decisión Andina 351 de 1993, "régimen común sobre derecho de autor y derechos conexos".
- Ley 527 de 1999, "por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las SSF es de certificación y se dictan otras disposiciones".
- Ley 594 de 2000, "por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones".
- Ley 850 de 2003, "por medio de la cual se reglamentan las veedurías ciudadanas".

6. ESTADO ACTUAL DE LA SSF RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

De acuerdo con el autodiagnóstico del Modelo de Seguridad y Privacidad de la Información de la Política Nacional de Gobierno Digital, el porcentaje de efectividad en la implementación de los controles de la Norma NTC/ISO 27001:2022 es de:

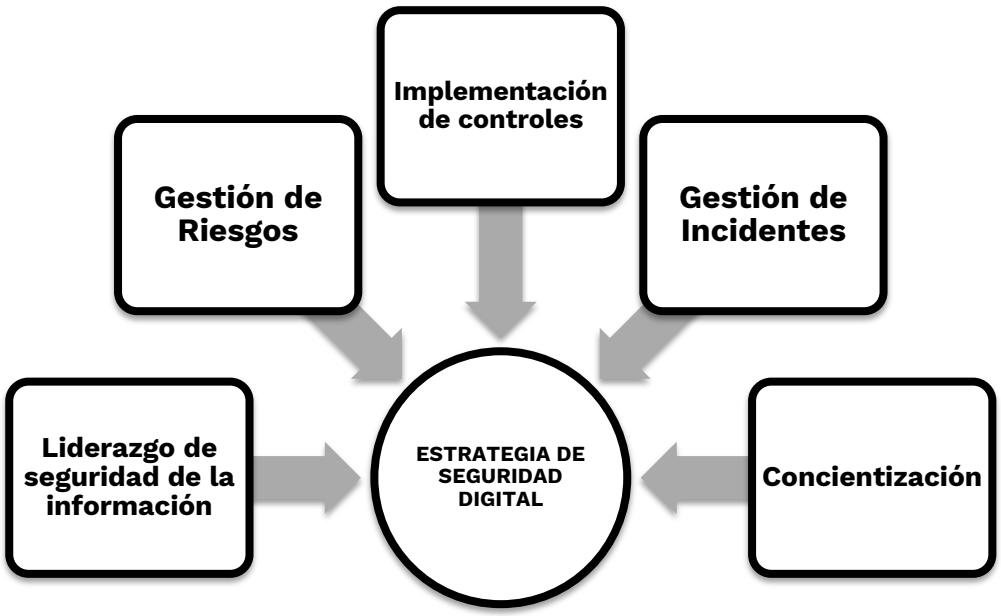
No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	Nivel de Madurez
A.5	CONTROLES ORGANIZACIONALES	47	100	EFECTIVO
A.6	CONTROLES DE PERSONAS	53	100	EFECTIVO
A.7	CONTROLES FÍSICOS	51	100	EFECTIVO
A.8	CONTROLES TECNOLÓGICOS	49	100	EFECTIVO
PROMEDIO EVALUACIÓN DE CONTROLES		50	100	EFECTIVO



7. ESTRATEGIA DE SEGURIDAD DIGITAL

LA SSF establecerá una estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, teniendo como premisa que dicha estrategia gira en torno a la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI, así como de la guía de gestión de riesgos de

Por tal motivo, ***LA SSF*** define las siguientes 5 estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad digital:



7.1. DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS (EJES)

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar, alineando las actividades a lo descrito dentro del MPSI y la resolución 500 de 2021:

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
Liderazgo de seguridad de la información	Asegurar que se establezca el Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de la política general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes dependencias y/o procesos de la SSF a través del establecimiento de los roles y responsabilidades en seguridad de la información.

Gestión de riesgos	Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados tendiendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.
Concientización	Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la SSF en seguridad y privacidad de la información.
Implementación de controles	Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la SSF, se pueden subdividir en controles tecnológicos y/o administrativos.
Gestión de incidentes	Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la SSF.

7.2. PORTAFOLIO DE PROYECTOS / ACTIVIDADES:

Para cada estrategia específica, **SSF** define los siguientes proyectos y productos esperados, que tienen por objetivo lograr la implementación y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI):

Iniciativa	Proyecto	Indicador	Actividades
Fortalecimiento de las capacidades institucionales para la seguridad y Privacidad de la Información	Fortalecimiento del Modelo de gestión de seguridad y privacidad de la información.	Documentar la política general de seguridad de la información aprobada y publicada.	Aprobar por el comité de gestión y desempeño la política general de seguridad de la información
		Documentar los indicadores de gestión para evaluar la eficacia operativa del MSPI	Apoyar en la consolidación de las actividades del MSPI.

		Matriz de activos de información actualizada y publicada.	Apoyar en la consolidación de activos de información, con relación a la responsabilidad de las funciones del Arquitecto de seguridad de la información.
		Matriz de riesgos de seguridad de la información actualizada y publicada.	Apoyar en la consolidación de la matriz de riesgos de seguridad de la información, con relación a la responsabilidad de las funciones del Arquitecto de seguridad de la información.
		Actualización de la declaración de aplicabilidad.	Apoyar en la consolidación de la declaración de aplicabilidad, con relación a la responsabilidad de las funciones del Arquitecto de seguridad de la información.
		Realizar seguimiento a los informes de vulnerabilidades asociados a SGSI.	Apoyar en la consolidación de las actividades de riesgos asociado a las vulnerabilidades tecnológicas, con relación a la responsabilidad de las funciones del Arquitecto de seguridad de la información.
		Apoyar la Definición de mecanismos para el Análisis de Vulnerabilidades y/o Pentest.	Apoyar en la consolidación de las actividades de riesgos asociado a las vulnerabilidades tecnológicas, con relación a la responsabilidad de las funciones del Arquitecto de seguridad de la información.
	Fortalecimiento del plan de Continuidad de	Porcentaje de avance en la documentación y apropiación del Plan de	FASE 1: Definir alcance Establecer roles

	la operación de los servicios de la SSF	Recuperación de Desastres	FASE 2: Análisis BIA Definición RTO-RPO Riesgos tecnológicos
			FASE 3: Definir estrategias de respaldo Definir estrategias de recuperación tecnológicas
			FASE 4: Documentación de procedimientos Plan de comunicaciones Manual de crisis Protocolos de recuperación
			FASE 5: Pruebas de DRP
	Fortalecimiento de las estrategias de Cambio, Cultura y Apropiación del Sistema de Gestión de Seguridad de la Información.	Nivel de apropiación institucional en Seguridad y Privacidad de la Información	Implementar el plan de cambio y cultura en Seguridad y Privacidad de la Información.

7.3. CRONOGRAMA DE ACTIVIDADES / PROYECTOS:

El responsable de seguridad de la información, con base a los proyectos definidos en la sección anterior, deberá establecer un cronograma de actividades donde se evidencie como se llevarán a cabo cada uno de los proyectos previstos. Las actividades podrán desarrollarse de forma secuencial o paralela según se considere.

Gestión	Actividad	Frecuencia	Responsable	Fecha Inicio	Fecha Final
Fortalecimiento del Modelo de gestión de seguridad y privacidad de la información.	Fortalecimiento del Modelo de gestión de seguridad y privacidad de la información.	Documentar la política general de seguridad de la información aprobada y publicada	Aprobar por el comité de gestión y desempeño la política general de seguridad de la información	1/02/2026	25/02/2026
		Documentar los indicadores de gestión para evaluar la eficacia operativa del MSPI	Apoyar en la consolidación de las actividades del MSPI	1/02/2026	25/02/2026
		Matriz de activos de información actualizada y publicada.	Apoyar en la consolidación de activos de información, con relación a la responsabilidad de las funciones del Arquitecto de seguridad de la información.	1/02/2026	30/03/2026

		Matriz de riesgos de seguridad de la información actualizada y publicada.	Apoyar en la consolidación de la matriz de riesgos de seguridad de la información, con relación a la responsabilidad de las funciones del Arquitecto de seguridad de la información.	1/04/2026	30/06/2026
		Actualización de la declaración de aplicabilidad	Apoyar en la consolidación de la declaración de aplicabilidad, con relación a la responsabilidad de las funciones del Arquitecto de seguridad de la información.	1/07/2026	30/07/2026
		Realizar seguimiento a los informes de vulnerabilidades asociados a SGSI	Apoyar en la consolidación de las actividades de riesgos asociado a las vulnerabilidades tecnológicas, con relación a la responsabilidad de las funciones del Arquitecto de seguridad de la información.	1/01/2026	31/12/2026

		Apoyar la Definición de mecanismos para el Análisis de Vulnerabilidades y/o Pentest	Apoyar en la consolidación de las actividades de riesgos asociado a las vulnerabilidades tecnológicas, con relación a la responsabilidad de las funciones del Arquitecto de seguridad de la información.	1/01/2026	31/12/2026
Fortalecimiento del plan de Continuidad de la operación de los servicios de la SSF	Fortalecimiento del plan de Continuidad de la operación de los servicios de la SSF	Porcentaje de avance en la documentación y apropiación del Plan de Recuperación de Desastres	FASE 1: Definir alcance Establecer roles	1/04/2026	30/04/2026
			FASE 2: Análisis BIA Definición RTO-RPO Riesgos tecnológicos	1/04/2026	30/05/2026
			FASE 3: Definir estrategias de respaldo Definir estrategias de recuperación tecnológicas	1/06/2026	30/07/2026
			FASE 4: Documentación de procedimientos Plan de comunicaciones Manual de crisis Protocolos de recuperación	30/08/2026	30/10/2026

			FASE 5: Pruebas de DRP	1/11/2026	15/12/2026
Fortalecimiento de las estrategias de Cambio, Cultura y Apropiación del Sistema de Gestión de Seguridad de la Información.	Fortalecimiento de las estrategias de Cambio, Cultura y Apropiación del Sistema de Gestión de Seguridad de la Información.	Nivel de apropiación institucional en Seguridad y Privacidad de la Información	Implementar el plan de cambio y cultura en Seguridad y Privacidad de la Información.	1/02/2026	31/12/2026