PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
Vigencia 2022

Departamento Administrativo para la Prosperidad Social
Bogotá, 2022

Contenido

1 INTRODUCCIÓN

Teniendo en cuenta la Política de Gobierno Digital como un componente del Modelo Integrado de Planeación y Gestión MIPG, la entidad acogiendo los lineamientos y mejores prácticas establecidas en diferente Normatividad y para la Vigencia 2022 realizará las actividades descritas en el presente plan, el cual forma parte integral del Plan de Acción Institucional de Prosperidad Social.

El Departamento Administrativo para la Prosperidad Social, ha identificado como su mayor activo la información, por consiguiente se encuentra en el proceso de dar continuidad a la mejora del Sistema de Gestión de Seguridad de la Información - SGSI, el cual le permite preservar la confidencialidad, integridad, trazabilidad y disponibilidad de la información, dando cumplimiento normativo a la legislación, políticas y lineamientos relacionados con la administración y protección de información, que aplican a las entidades estatales.

2 OBJETIVO

Definir el plan de seguridad y privacidad de la información, el cual forma parte integral del Plan de Acción Institucional de Prosperidad Social para la vigencia de 2022, con el fin de preservar los criterios de confidencialidad, integridad, disponibilidad, trazabilidad y privacidad de la información en Prosperidad Social.

3 DEFINICIONES Y SIGLAS

Activo de Información: Se entiende por todo aquel elemento lógico o físico que conforme cualquiera de los sistemas de información de la Entidad. Ej. Información de bases de datos, programas de computación, plataforma tecnológica (procesamiento de datos o comunicaciones), documentos impresos y Recursos Humano y que tienen un valor para la entidad.

Colaborador: Servidor público, Contratista, pasante, proveedor y en general cualquier persona que tenga nexo con la entidad y tenga acceso a información de la misma.

Confidencialidad: Asegurar que la información está disponible solamente para los usuarios autorizados a tener acceso a dichos datos.

Control: Una forma para manejar el riesgo, incluyendo políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas, y que pueden ser de carácter administrativo, técnico o legal.

Criptografía: Técnica de cifrado, es decir de escribir con clave secreta o de un modo enigmático, con el fin de conservar la confidencialidad de la información.

Disponibilidad: Asegurar que los usuarios tengan, en todo momento, la información a la cual tienen derecho.

Información: es un conjunto organizado de datos. Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas etc.

Integridad: Asegurar que la información es adecuada y apropiada para su procesamiento.

Política: Definición, orientación o directriz de alto nivel que refiere la posición de la entidad sobre un tema específico.

Seguridad de la Información: Salvaguardar la confidencialidad, integridad y disponibilidad de la información.

Sistema de Gestión de Seguridad de la Información (SGSI): Conjunto de procesos que permiten conservar los principios de seguridad de la información, estableciendo las políticas y objetivos a alcanzar por una organización, con un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Terceros: Se entiende por tercero a toda persona, jurídica o natural, como proveedores, contratistas o consultores, que provean servicios o productos a la Entidad, o entre los cuales medie convenio, contrato o relación alguna.

Usuario: colaborador que hace uso de un equipo computacional o de un sistema de información.

SIGLAS

DPS: Departamento Administrativo para la Prosperidad Social

MSPI: Modelo de Seguridad y Privacidad de la Información

MIPG: Modelo Integrado de Planeación y Gestión

SGSI: Sistema de Gestión de Seguridad de la Información

SGC: Sistema de Gestión de Calidad
ISO: International Organization for Standardization (Organización Internacional de Normatización)

4 REFERENCIAS NORMATIVAS

- ✓ **CONPES 3995 DE 2020:** Política Nacional de Confianza y Seguridad Digital
- ✓ **NORMA ISO 27001- 2013:** Es un estándar para los Sistemas Gestión de la Seguridad de la Información que permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.
- ✓ **Ley 1273 de 2009** "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".
- ✓ **Ley 1712 de 2014** "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".
- ✓ **Ley 1581 de 2012** "Por la cual se dictan disposiciones generales para la protección de datos personales".
- ✓ **Ley 734 de 2002** "Por la cual se expide el Código Disciplinario Único". Articulo 34 deberes del servidor público., Esta ley quedará derogada a partir del 29/03/2022. El plazo de entrada en vigencia de la Ley 1952 de 2019 (Art. 265) se prorroga hasta el 29 de marzo de 2022 por el artículo 73 de la Ley 2094 de 2021
- ✓ **Ley 1952 de 2019: "**Por medio de la cual se expide el código general disciplinario se derogan la ley 734 de 2002 y algunas disposiciones de la ley 1474 de 2011, relacionadas con el derecho disciplinario. El plazo de entrada en vigencia de la Ley 1952 de 2019 (Art. 265) se prorroga hasta el 29 de marzo de 2022 por el artículo 73 de la Ley 2094 de 2021
- ✓ **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".
- ✓ **Decreto 103 de 2015** "Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones"
- ✓ **Decreto 1078 de 2015** "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".
- ✓ **Decreto 1377 de 2013** "Por el cual se reglamenta parcialmente la Ley 1581 de 2012"

5 ROLES Y RESPONSABILIDADES

Los roles y responsabilidades para la seguridad de la información de la entidad se describen a continuación:

Rol	Responsabilidades de seguridad de la información
COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO	Responsable de revisar y aprobar la implementación de la política general del SGSI. Responsable de la Revisión por la Dirección del Sistema de Gestión de Seguridad de la Información SGSI.
GRUPO INTERNO DE TRABAJO - GOBIERNO DE TECNOLOGÍAS DE LA INFORMACIÓN	Encargado de la implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información SGSI, con el propósito de generar una cultura de la seguridad de la información en la entidad. Responsable de presentar los resultados del SGSI en la revisión por la Dirección ante el Comité Institucional de gestión y desempeño
OFICINA ASESORA DE PLANEACIÓN	Encargado de asesorar, orientar y apoyar a las Oficinas, Direcciones y Subdirecciones de la entidad, en los temas relacionados con la realización, actualización o ajustes de los procedimientos, procesos, guías, formatos y manuales para alinearlos con el Sistema de Gestión de Calidad - SGC y el Sistema de Gestión de Seguridad de la Información – SGSI. De igual manera orientarlas en la Administración del Riesgo, realizando la revisión, análisis y consolidación de la información.
SUBDIRECCIÓN DE TALENTO HUMANO	Responsable de notificar a los funcionarios de la entidad el cumplimiento de la política de seguridad de la Información del SGSI, por medio del (Acuerdo Individual de Confidencialidad (F-GTI-6)) y de las capacitaciones de inducción de la Entidad. Encargados de notificar las novedades de los empleados, en relación con la creación, modificación o cancelación de estos en el directorio activo, por ende, permisos de acceso a correo electrónico y a la información de la entidad.
GRUPO INTERNO DE TRABAJO –	Responsable de seguir con los lineamientos establecidos en la política, implementando los controles de Seguridad Informática a que haya lugar en los recursos de tecnologías de información y comunicaciones.

INFRAESTRUCTURA Y SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN	Encargados de atender los incidentes de seguridad informática, supervisar las acciones de los proveedores de servicios de tecnología que tengan a cargo y determinar el inventario de activos de información y recursos tecnológicos propios o que tengan en custodia.
SUBDIRECCIÓN DE CONTRATACIÓN	Encargado de la inclusión y supervisión de cláusulas de seguridad de información en los contratos y verificación de los acuerdos de niveles de servicio; dicta lineamientos para que se reporte oportunamente el retiro de colaboradores.
SUBDIRECCIÓN DE OPERACIONES	Encargado de la seguridad y accesos físicos en cada una de las sedes de la Entidad y gestionar los incidentes de seguridad de la información que no sean informáticos.
OFICINA ASESORA JURÍDICA	Brindar asesoría legal a la entidad, en lo que refiere al cumplimiento de la normativa de Seguridad de la Información, protección de datos personales, transparencia y acceso a la información pública, entre otras.
OFICINA CONTROL INTERNO	Responsables de realizar la evaluación y seguimiento al cumplimiento de las políticas, lineamientos y requisitos de Seguridad de la información, así como auditar el SGSI y presentar los hallazgos.
COLABORADORES	Todos los colaboradores de la entidad deberán aplicar y cumplir con las políticas, lineamientos, procesos, procedimientos referentes a Seguridad de la Información, así como asistir a las sensibilizaciones o capacitaciones del SGSI.

6 SITUACIÓN ACTUAL

La entidad identifica el nivel de madurez en la implementación del Modelo de seguridad y Privacidad de la Información, a través del diligenciamiento del instrumento de evaluación del (MSPI) diseñado por el MINTIC, el cual permite:

- Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.
- Determinar el nivel de madurez de los controles de seguridad de la información, obteniendo la brecha en el cumplimiento de los controles técnicos de la ISO 27001.

Primero se evaluaron los controles administrativos de la norma ISO 27001, los cuales se mencionan a continuación:

- POLITICAS DE SEGURIDAD DE LA INFORMACIÓN
- ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
- SEGURIDAD DE LOS RECURSOS HUMANOS

- GESTIÓN DE ACTIVOS
- ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO
- CUMPLIMIENTO
- RELACIONES CON LOS PROVEEDORES

Posteriormente se realiza la evaluación de los controles técnicos de la norma, los cuales se mencionan a continuación.

- CONTROL DE ACCESO
- CRIPTOGRAFÍA
- SEGURIDAD FÍSICA Y DEL ENTORNO
- SEGURIDAD DE LAS OPERACIONES
- SEGURIDAD DE LAS COMUNICACIONES
- ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS
- GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Realizado por completo el ejercicio se cuenta con el resultado del diagnóstico del estado de la implementación y madurez del Modelo de Seguridad y Privacidad de la Información en Prosperidad social, con vigencia 2022, obteniendo los resultados de medición que se muestran a continuación.

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	63	100	GESTIONADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	92	100	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	79	100	GESTIONADO
A.9	CONTROL DE ACCESO	74	100	GESTIONADO
A.10	CRIPTOGRAFÍA	60	100	EFECTIVO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	86	100	OPTIMIZADO
A.12	SEGURIDAD DE LAS OPERACIONES	74	100	GESTIONADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	72	100	GESTIONADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	61	100	GESTIONADO
A.15	RELACIONES CON LOS PROVEEDORES	90	100	OPTIMIZADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	83	100	OPTIMIZADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	80	100	GESTIONADO
A.18	CUMPLIMIENTO	79	100	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES		78	100	GESTIONADO

7 PLAN DE TRABAJO

Teniendo en cuenta el resultado del análisis del estado actual de la implementación y madurez del Modelo de Seguridad y Privacidad de la información y basados en la norma ISO 27001:2013, se establece el siguiente plan para la implementación del Modelo de Seguridad y Privacidad de la Información.

7.1 OBJETIVOS ESPECIFICOS DEL PLAN

- Proteger los activos de información, con base en los criterios de confidencialidad, integridad y disponibilidad.
- Gestionar los riesgos de seguridad digital para mantenerlos en niveles aceptables.
- Sensibilizar a los servidores públicos y contratistas de la Entidad acerca del Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información, fortaleciendo el nivel de conciencia de los mismos, en cuanto a la necesidad de salvaguardar los activos de información críticos de la Entidad.
- Monitorear el cumplimiento de los requisitos, directrices y políticas de seguridad de la información.
- Implementar la mejora continua para el Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información de Gobierno Digital"

7.2 INDICADOR

- Nombre del Indicador: Estado de madurez de la Seguridad y Privacidad de la Información de la Entidad.
- Medición: Aplicación del instrumento de madurez de MINTIC

7.3 ACTIVIDADES DEL PLAN DE TRABAJO

No	ACTIVIDAD	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	FECHA
1	ESTRUCTURAR EL NUEVO ALCANCE DEL SGSI	Continuar la implementación del alcance SGSI establecido en el Manual de SGSI M-GTI-1 de la Entidad para la Fase 3 que cubre nuevos Procesos estratégicos y componentes de equidad digital para la vigencia de 2022,	1. GRUPO INTERNO DE TRABAJO - GOBIERNO DE TECNOLOGÍAS DE LA INFORMACIÓN 2. OFICINA ASESORA DE PLANEACIÓN	Enero de 2022

No	ACTIVIDAD	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	FECHA
2.	APROBACIÓN DEL NUEVO ALCANCE DEL SGSI	Aprobación del nuevo alcance del SGSI en el marco del Comité Institucional de Gestión y desempeño	1. COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO	Según programación del Comité Institucional
3	REVISAR Y ACTUALIZAR LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Revisar y actualizar la política del SGSI; así como, de las catorce (14) políticas específicas de seguridad de la Información para la Entidad,	1. GRUPO INTERNO DE TRABAJO - GOBIERNO DE TECNOLOGÍAS DE LA INFORMACIÓN	Febrero de 2022
4	APROBACIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Revisar y aprobar las políticas de seguridad actualizadas en el marco del Comité Institucional de Gestión y desempeño	1. COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO	Según programación del Comité Institucional
5	MEJORA CONTINUA DEL SGSI	Trabajar en la mejora continua del Sistema de Gestión de Seguridad de la Información SGSI, tomando como entradas: - Las oportunidades de mejora de la auditoría interna al SGSI de 2021, y auditoría externa de seguimiento SGSI de 2021 - El autodiagnóstico de los controles técnicos	1. GRUPO INTERNO DE TRABAJO - GOBIERNO DE TECNOLOGÍAS DE LA INFORMACIÓN	marzo a junio de 2022
6	GESTIÓN DEL RIESGO DE SEGURIDAD DIGITAL	Realizar la implementación de las actividades definidas en el Plan de Tratamiento de Riesgos. Generar la alineación de la gestión de riesgo de seguridad digital con la	1. GRUPO INTERNO DE TRABAJO - GOBIERNO DE TECNOLOGÍAS DE LA INFORMACIÓN 2. OFICINA ASESORA DE PLANEACIÓN	Enero a diciembre de 2022

No	ACTIVIDAD	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	FECHA
		nueva guía de gestión del riesgo de Función Pública. Implementar los controles requeridos para la mitigación de riesgos de seguridad digital identificados, tomando como base los controles del Anexo A de la norma ISO 27001:2013 Actualizar la declaración de aplicabilidad SoA.		
7	AUDITORIA DE SEGURIDAD DE LA INFORMACIÓN A LOS PROVEEDORES	Auditar el cumplimiento de requisitos de seguridad de la información a los proveedores que de acuerdo con la relación contractual tienen gestión de los activos de información de Prosperidad Social	1. SUPERVISORES DE CONTRATO 2. GRUPO INTERNO DE TRABAJO - GOBIERNO DE TECNOLOGÍAS DE LA INFORMACIÓN	Febrero a Noviembre de 2022
8	DEFINIR Y EJECUTAR EL PLAN DE COMUNICACIONES DEL SGSI	Definir las actividades que permitan fomentar la cultura de seguridad y privacidad de la información y la apropiación de las políticas y lineamientos del SGSI.	1. GRUPO INTERNO DE TRABAJO - GOBIERNO DE TECNOLOGÍAS DE LA INFORMACIÓN	Enero a diciembre de 2022
9	EJECUCIÓN DEL PLAN DE PRUEBAS DEL PLAN DE CONTINGENCIA TECNOLÓGICA	Ejecutar el plan pruebas definido para confirmar le eficacia de las estrategias de contingencia tecnológica propuestos para garantizar la continuidad de las aplicaciones, sistemas de información y servicios críticos que soportan la operación de los procesos	1. GRUPO INTERNO DE TRABAJO – INFRAESTRUCTURA Y SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN	Febrero a Diciembre de 2022

No	ACTIVIDAD	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	FECHA
		misionales de Prosperidad Social.		
10	REALIZAR LA MEDICIÓN CON LOS INDICADORES DEL SGSI	Analizar el estado de cumplimiento de los objetivos del SGSI a través de los resultados de los indicadores propuestos.	2. GRUPO INTERNO DE TRABAJO - GOBIERNO DE TECNOLOGÍAS DE LA INFORMACIÓN	Enero a diciembre de 2022
11	ACTUALIZACIÓN DEL INVENTARIO DE ACTIVOS DE INFORMACIÓN	Actualizar el inventario de activos de información y extenderlo según el nuevo alcance de la fase 3 del SGSI	1. GRUPO INTERNO DE TRABAJO - GOBIERNO DE TECNOLOGÍAS DE LA INFORMACIÓN	Junio a agosto de 2022
12	ACTUALIZACIÓN DE PROCEDIMIENTOS DEL SGSI y VALIDACIÓN DE LOS REGISTROS DE EJECUCIÓN DE ESTOS.	Revisar y actualizar los procedimientos relacionados con el SGSI; así como la validación de existencia e idoneidad de los registros producto de la ejecución de estos procedimientos: ▪ PROCEDIMIENTO DE CREACIÓN, MODIFICACIÓN Y CANCELACIÓN DE CUENTAS DE USUARIOS ▪ PROCEDIMIENTO PARA LA GESTIÓN DE LA CAPACIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA	1. GRUPO INTERNO DE TRABAJO - GOBIERNO DE TECNOLOGÍAS DE LA INFORMACIÓN **2.** GRUPO INTERNO DE TRABAJO – INFRAESTRUCTURA Y SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN	FEBRERO A JULIO DE 2022

No	ACTIVIDAD	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	FECHA
		▪ PROCEDIMIENTO GESTIÓN DE VULNERABILIDADES ▪ PROCEDIMIENTO DE REVISIÓN DE SOFTWARE INSTALADO EN LOS EQUIPOS DE CÓMPUTO ▪ MANUAL DE GESTIÓN DE ACTIVOS DE INFORMACIÓN ▪ PROCEDIMIENTO NOTIFICACIÓN Y GESTIÓN DE EVENTOS E INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN ▪ PROCEDIMIENTO GESTIÓN DE CAMBIOS ▪ MANUAL DE BACKUPS Y RECUPERACIÓN PARA LA INFRAESTRUCTURA TECNOLÓGICA ▪ PROCEDIMIENTO SOLICITUD DE PERMISOS DE ADMINISTRADOR LOCAL DEL EQUIPO ▪ GUÍA PARA EL BORRADO SEGURO DE INFORMACIÓN ▪ GUÍA DE CIFRADO Y DESCIFRADO DE INFORMACIÓN ▪ MANUAL PARA LA GESTIÓN Y TRAZABILIDAD DE LOGS		

No	ACTIVIDAD	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	FECHA
13	AUDITORIA INTERNA AL SGSI	Evaluar el cumplimiento de los requisitos establecidos, implementados y de Mejora continua del Sistema de Gestión y Seguridad de información (SGSI)	1. OFICINA CONTROL INTERNO	Agosto de 2022
14	MONITOREO DEL CUMPLIMIENTO DE LAS POLITICAS DE SEGURIDAD	Evaluar el cumplimiento de las directrices establecidas en cada una de las 14 políticas específicas de seguridad de la información	1. GRUPO INTERNO DE TRABAJO - GOBIERNO DE TECNOLOGÍAS DE LA INFORMACIÓN	FEBRERO A NOVIEMBRE DE 2022
15	APLICAR SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS	Integrar en la gestión de proyectos de la organización, que los riesgos de seguridad de la información se identifiquen y traten como parte de los proyectos.	1. GRUPO INTERNO DE TRABAJO - GOBIERNO DE TECNOLOGÍAS DE LA INFORMACIÓN 2.	FEBRERO A JULIO DE 2022