PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Departamento Administrativo para la Prosperidad Social.
Bogotá D.C. – Colombia.
Enero 2021

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 2021 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 implementación 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.

OBJETIVO DEL PLAN

Definir el plan de seguridad y privacidad de la información para el año 2021, el cual forma parte integral del Plan de Acción Institucional de Prosperidad Social, para preservar los criterios de confidencialidad, integridad, disponibilidad, trazabilidad y privacidad de la información en Prosperidad Social.

OBJETIVOS DE LA POLITICA DE SEGURIDAD DE LA INFORMACIÓN

Los objetivos de la Política de Seguridad de la Información del Departamento Administrativo para la Prosperidad Social son los siguientes.

1. Establecer mecanismos para asegurar los activos de Información, la correcta administración y protección de los datos en la Entidad.
2. Incrementar la integridad, confidencialidad, disponibilidad y trazabilidad de la información, mediante controles que eviten el uso inadecuado de la misma por parte de personas, procesos y otros que puedan afectar la gestión e imagen de la Entidad.
3. Proteger la infraestructura tecnológica y los datos contenidos en ella mediante controles tecnológicos, recursos físicos y financieros necesarios para su ejecución y sostenimiento.
4. Prevenir y mitigar los incidentes de Seguridad de la Información en Prosperidad Social.
5. Incrementar mecanismos de comunicación que contribuyan al fortalecimiento de la cultura de la seguridad de la información entre los servidores públicos de Prosperidad Social.

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)

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 perderá su vigencia, a partir del 1 de julio de 2021 de conformidad con el artículo 140 de la Ley 1955 de 2019, la cual prorrogó la vigencia de la Ley 1952 de 2019, cuyo artículo 265 deroga la Ley 734 de 2002.
- ✓ **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.
- ✓ **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"

1. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Dirección del Departamento Administrativo para la Prosperidad Social (DPS), entiende la importancia de una adecuada gestión de la información, por lo tanto, se compromete con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la Entidad.

Para Prosperidad Social, la protección de la información es de vital importancia y se empeña en la disminución del impacto generado sobre sus activos de información, por los riesgos e incidentes identificados de manera sistemática, con el objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad, disponibilidad y trazabilidad de la información.

El Departamento Administrativo *p*ara la Prosperidad Social se compromete en determinar y documentar los controles, los procedimientos y normas de seguridad, los cuales deben ser de estricto cumplimiento por todos los servidores públicos, terceros y grupos de interés, que tienen accesos a la información, y aplicar las normas establecidas cuando se infringen las políticas de seguridad de la información.

Con base en lo anterior, establece los siguientes componentes para la implementación de la política de seguridad y privacidad del SGSI en la entidad:

1.1 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

El Departamento Administrativo para la Prosperidad Social estructura las responsabilidades para la gestión de la seguridad de los activos de información, claramente separadas y asignadas, incluyendo el Comité institucional de Gestión y Desempeño

1.2 SEGURIDAD EN LOS RECURSOS HUMANOS

El Departamento Administrativo para la Prosperidad Social se compromete en establecer y mantener la responsabilidad del funcionario, contratista o tercero por el manejo seguro y adecuado sobre los activos de información, la cual se extiende aún después de finalizada la relación laboral o contractual; también garantiza el entendimiento de lo anterior, mediante la debida instrucción, socialización y suscripción de acuerdos de confidencialidad.

1.3 GESTIÓN DE ACTIVOS

Los activos de información son inventariados, revisados periódicamente y asignados a un responsable; sobre estos activos se establecen niveles de protección, acceso y procedimientos para su utilización.

1.4 CONTROL DE ACCESO

El Departamento Administrativo para la Prosperidad Social establece las medidas de control de acceso a nivel de red, sistema operativo, Base de Datos, aplicaciones y acceso físico que garantice la eficiencia, eficacia y efectividad de la seguridad.

Prosperidad Social se reserva el derecho de monitoreo a fin de identificar de manera inequívoca cada usuario y el uso debido de los Activos de Información.

Los roles y responsabilidades de los usuarios de las áreas o procesos están debidamente diferenciadas para reducir las oportunidades de alteración a los activos de información.

1.5 CRIPTOGRAFÍA

El Departamento Administrativo para la Prosperidad Social utiliza para la protección de los activos de información, claves, aplicaciones e igualmente fomenta su uso para todas las situaciones y comunicaciones que involucren datos sensibles y demás que considere relevante.

1.6 SEGURIDAD FÍSICA Y AMBIENTAL

El Departamento Administrativo para la Prosperidad, cuentan con protecciones físicas y ambientales acordes con la clasificación de los activos de información que protegen el almacenamiento y procesamiento de la información, perímetros de seguridad, controles de acceso físicos, controles especiales de áreas de mayor sensibilidad, seguridad de los equipos, seguridad en el suministro eléctrico y cableado, condiciones ambientales de operación y sistemas de contención, detección y extinción de incendios, que preservan el medio ambiente.

Se garantizan los protocolos de seguridad de la información en condiciones de mantenimiento, traslado, eliminación o cuando los equipos se den de baja.

A todo medio de almacenamiento o centro de procesamiento de terceros, que procese o almacene información de Prosperidad Social, se le exige cumplir con la seguridad física y tecnológica requerida con el propósito de mantener la disponibilidad, integridad, confidencialidad y trazabilidad de la información.

1.7 SEGURIDAD EN LAS OPERACIONES

Los procedimientos y responsabilidades de administración y seguridad pertinentes a cada ambiente tecnológico están documentados, de forma que garantice una debida gestión de cambios, el seguimiento a los estándares de seguridad definidos y la atención de incidentes de seguridad que se presenten.

La planificación y aprobación de los sistemas de información son adecuados y consideran las necesidades futuras, al igual que la seguridad en el intercambio de información, mediante controles que garanticen su confidencialidad, integridad, disponibilidad y trazabilidad, así mismo provee protección contra software malicioso.

1.8 SEGURIDAD DE LAS COMUNICACIONES

El Departamento Administrativo para la Prosperidad Social, asegura la protección adecuada de la información que se transmite en las redes y comunicaciones que utiliza la entidad, para reducir los riesgos de la modificación y uso no autorizado de los activos de información.

1.9 ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

El Departamento para la Prosperidad Social realiza análisis e implementación de los requerimientos de seguridad en los sistemas de información desarrollados internamente y/o adquiridos, que incluyen validación de usuarios, datos de entrada y salida y el procesamiento de los mismos.

Los responsables de los sistemas de información deben considerar los requerimientos de seguridad necesarios para mantener la integridad y confidencialidad, en la etapa temprana del desarrollo y la incorporación de controles relevantes.

1.10 RELACIONES CON PROVEEDORES

El Departamento Administrativo para la Prosperidad Social establecerá e implementará los lineamientos y controles para que los proveedores y contratistas realicen un adecuado manejo de la información acorde al modelo de seguridad de la Información, estableciendo un marco de colaboración equilibrado de manera de que se preserve la confidencialidad, integridad y disponibilidad de los datos de la Entidad

1.11 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

El Departamento Administrativo Para la Prosperidad Social promueve la debida gestión a los incidentes de Seguridad de la información, siguiendo procedimientos apropiados, para su manejo, atención y evaluación del impacto causado.

Todo funcionario, contratista o tercero que tenga un vínculo contractual o acceda a la información de Prosperidad Social debe reportar como incidente de seguridad cualquier anomalía o mal uso de los activos de información.

1.12 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DENTRO DE LA CONTINUIDAD DEL NEGOCIO

El Departamento Administrativo para la Prosperidad Social realiza los planes de continuidad en aquellos procesos que son críticos para su operación y supervivencia. Estos planes deben considerar medidas técnicas, administrativas y de vínculo con instituciones externas.

Los planes se deben probar y revisar periódicamente y están articulados en toda la empresa con recursos tecnológicos y no tecnológicos.

1.13 CUMPLIMIENTO DE LOS REQUISITOS LEGALES

El Departamento Administrativo para la Prosperidad Social cumple con los requisitos legales internos y externos aplicables a la Seguridad de la Información que gestiona, incluye entre otros los derechos de propiedad intelectual, protección de datos personales, tiempos de retención de registros, privacidad de información, uso debido de los recursos de procesamiento, uso de criptografía y recolección de evidencia y auditorías.

Prosperidad Social garantiza que todo el software instalado en la organización cumple con la ley de derechos de autor y la normatividad vigente.

2 ROLES Y RESPONSABILIDADES

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

2.1 COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO

Responsable de revisar y aprobar la implementación de la política general del SGSI.

2.2 GRUPO INTERNO DE TRABAJO - GOBIERNO DE TECNOLOGÍAS DE LA INFORMACIÓN

Responsable de presentar ante el Comité Institucional de Gestión y Desempeño la documentación, estrategia y propuestas para el mantenimiento y fortalecimiento del SGSI.

Encargo de la implementación, mantenimiento y mejora continua del SGSI, con el propósito de generar una cultura de la seguridad de la información en la entidad.

2.3 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.

2.4 GRUPO INTERNO DE TRABAJO – INFRAESTRUCTURA Y SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN

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.

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.

2.5 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 (F-DE-11-Acuerdo de confidencialidad y Manejo de la Información) 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.

2.6 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.

2.7 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.

2.8 OFICINA ASESORA JURÍDICA

Brindar asesoría legal a la entidad, en lo que refiere al cumplimiento de la normatividad de Seguridad de la Información, protección de datos personales, transparencia y acceso a la información pública, entre otras.

2.9 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.

2.10 GRUPO INTERNO DE TRABAJO - PARTICIPACIÓN CIUDADANA

Responsable de gestionar o direccionar los PQRS que lleguen a la entidad dentro de los términos legales vigentes.

- Ley 1581 de 2012 y Decreto 1377 de 2013.
- Ley 1266 de 2008

2.11 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.

3. IMPLEMENTACIÓN DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para esta etapa del proyecto se pretende de acuerdo al modelo MSPI del Ministerio de Tecnologías de Información, el MIPG del Departamento Administrativo de la Función Pública y basados en la norma ISO 27001:2013, Continuar la implementación del SGSI de acuerdo con lo establecido en el alcance del Manual de SGSI de la Entidad para la Fase 2 que cubre Procesos misionales y estratégicos priorizados para el año 2021 incluidos en Equidad Digital, aplicando el ciclo de vida de los procesos - PHVA Planear, Hacer, Verificar y Actuar e incluyendo los Objetivos de Control y controles establecidos en el Anexo A de la referida Norma.

Con el objetivo de continuar con las actividades iniciadas en el año 2020 se continuará con la implementación del sistema de gestión de seguridad en la Entidad, para lo cual en la vigencia 2021 se proyecta continuar en la implementación del modelo de seguridad y se realizarán las siguientes actividades:

- Implementar el Plan de tratamiento de riesgos aprobado por los responsables de los procesos.
- Implementar Controles establecidos en la declaración de Aplicabilidad
- Ejecutar los Planes de Recuperación ante desastres DRP.

Posteriormente se priorizarán los riesgos, se consolidarán los hallazgos y se plantearán las principales acciones que deben ser realizadas por la Entidad para mitigar de una manera efectiva todo el conjunto de riesgos que pueden materializar afectación a la información sensible manejada por la entidad dentro del alcance definido del sistema. Los posibles elementos que puede contener este plan serán los siguientes:

- Riesgos y/o hallazgos de no cumplimiento que van a ser mitigados
- Selección de controles a aplicar para mitigación del riesgo.
- Acciones a seguir para llevar a cabo la implementación de los controles.
- Tiempos estimados de implementación
- Recursos necesarios a involucrar en la implementación de los controles
- Costos estimados de implementación

Se continuará con la actualización de los procedimientos de seguridad básicos para soportar el SGSI.

Así mismo, se actualizarán y elaborarán formatos y procedimientos adicionales y que tienen como objetivo definir lineamientos y flujos de actividades para la implementación de las mejores prácticas en la Entidad, los cuales son:

- Gestión de recursos humanos
- Gestión de terceros
- Control de acceso físico
- Control de acceso lógico
- Mantenimiento, baja y reutilización de equipos y medios
- Capacitación, entrenamiento y concientización en seguridad de la información
- Gestión de la capacidad
- Separación de ambientes
- Control de versiones
- Monitoreo y revisión de logs
- Control de software
- Controles criptográficos
- Control de software malicioso
- Buen uso de los activos

En primera etapa se realizará la actualización y publicación de las Políticas y Lineamientos de seguridad de la Información para la Entidad, basados en la auditoría de certificación en la Norma ISO 27001:2013 realizada en el año 2020. De otra parte, se realizará un proceso de contratación para ampliar esta certificación a los procesos Misionales de la Entidad incluidos en Equidad Digital.

4. IMPLEMENTACION DEL PLAN DE TRATAMIENTO DE RIESGOS

Se realizará la implementación de las actividades definidas en el Documento Plan de Tratamiento de Riesgos.

Una vez definidas las acciones que deben ser llevadas a cabo para mitigar los riesgos que han sido identificados en la fase de diagnóstico y gestionando los recursos necesarios para las tareas de implementación del plan, se realizarán las acciones pertinentes.

AMPLIACIÓN DE LA CERTIFICACIÓN EN LA NORMA ISO 27001:2013

La Entidad pretende ampliar la certificación en la Norma ISO 27001:2013 este año y para lo cual es necesario la realización de una auditoría interna antes de llevar a cabo la del Ente certificador.

En la vigencia 2019 y 2020 se llevaron a cabo dos auditoría internas al Sistema de Gestión de Seguridad de la Información- SGSI y para este año, se solicitó una nueva auditoría interna antes de realizar el proceso de certificación por el Ente externo, actividad que se llevará a cabo de acuerdo a lo establecido en el PASI “Plan Anual de Auditorías, asesorías, acompañamientos, seguimientos e informes de Ley “ del año 2021.