FONDECUN

FONDO DE DESARROLLO DE PROYECTOS DE CUNDINAMARCA

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023

CUNDINAMARCA ¡REGIÓN Que Progresa!

Gobernación de Cundinamarca

Sede Administrativa
Av. Carrera 10 No. 28-49 Torre A, Piso 21
Teléfonos: 243 2328 / 243 2806

www.fondecun.gov.co
@fondecun

Contenido

1. INTRODUCCIÓN.

Dentro de la implementación de la política de gobierno digital y siguiendo el manual de la política expedido por el Ministerio de Tecnologías de información y de las Comunicaciones donde establece que la política tiene como propósito promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un estado y ciudadanos competitivos, proactivos e innovadores, que generen valor público en un entorno de confianza digital.

Y con el propósito de salvaguardar la información de la entidad en todos sus aspectos, garantizando la seguridad de los datos y el cumplimiento de las normas legales, se ha establecido el Plan de Seguridad y Privacidad de la información, que contiene los lineamientos operativos de gestión, administración y procedimientos de seguridad de la información, estableciendo las prácticas de seguridad aplicadas en la entidad, soportado en el Modelo de Seguridad y Privacidad de la información (MSPI), que 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, y de acuerdo al ámbito de aplicación del modelo Integrado de Planeación y Gestión.

Teniendo en cuenta que dentro de las organizaciones sin importar su área o contexto de desarrollo se presenta la información como uno de los activos más valiosos y primordiales, aportando en el desarrollo de cada proceso interno con el fin de cumplir los objetivos y alcanzar el éxito de la organización.

El aseguramiento y la protección de la seguridad de la información de las organizaciones y de los datos de carácter personal de los usuarios, representan un reto al momento de pretender garantizar su confidencialidad, integridad, disponibilidad y privacidad, razón por la cual, la seguridad de la información se ha convertido en uno de los aspectos de mayor preocupación a nivel mundial.

Por lo anterior, se actualiza el presente documento dando cumplimiento al Decreto 612 de 2018, actualizando el Plan de implementación de Seguridad y Privacidad de la Información.

2. NORMATIVIDAD

El plan estratégico de privacidad de la información se define teniendo en cuenta el siguiente marco normativo:

Decreto 1008 de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital, define la seguridad de la información como principio de la Política de Gobierno Digital
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 103 de 2015,	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
Decreto 1494 de 2015	Por el cual se corrigen yerros en la Ley 1712 de 2014
Manual gobierno en línea 3.1 ver 2014 – 06 - 12.	Para la Implementación de la Estrategia de Gobierno en Línea, entidades del orden nacional; Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea.
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.
Decreto 2573 de 2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581de 2012.
Decreto 2609 de 2012	Por el cual se reglamenta el Título V de la Ley 594 de 2000 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado".
Decreto 2693 de 2012	Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones.
Ley estatutaria 1581 de 2012.	Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República.
Ley 1266 de 2008	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales.

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.
Constitución Política de Colombia 1991 - Artículo 15	Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar.

3. DISPOSICIONES GENERALES DEL MANEJO DE LA INFORMACIÓN.

La presente política partiendo de la importancia de la seguridad y del derecho que tienen los titulares de la información, tiene en cuenta la ley 1266 de 2008, "*Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones*", con el fin de que se tenga derecho a conocer, actualizar y rectificar la información que se haya recogido sobre ellos en las bases de datos y archivos de la entidad.

4. OBJETIVO DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

4.1 Objetivo General

Definir las acciones para aportar a la implementación del Modelo de Seguridad y Privacidad de la información, permitiendo salvaguardar la confidencialidad, integridad y disponibilidad de la información en cumplimiento a la normatividad vigente, acorde a los requerimientos del modelo de seguridad de la estrategia de gobierno en línea, los requerimientos del negocio, desde el enfoque de la seguridad informática frente a ciberamenazas.

4.2 Objetivos Específicos

- Verificar los alcances establecidos en el Modelo de Privacidad y Seguridad de la Información (MPSI) y la documentación base con la que cuenta la entidad. Revisada esta documentación se realiza el cruce con los lineamientos establecidos en la Política de Gobierno Digital.
- Definir las etapas para establecer la estrategia de seguridad de la información de la entidad.
- Concientizar a todos los colaboradores, áreas, procesos, proveedores, externos en general sobre la necesidad e importancia de gestionar de manera adecuada, los riesgos inherentes a la gestión.

- Establecer los lineamientos, optimización e implementación de la política se Seguridad y Privacidad de la Información, que se deben aplicar en Fondecún.

- Involucrar y comprometer a todos en la formulación e implementación de controles y acciones encaminadas a prevenir y administrar los riesgos.

- Establecer, mediante una adecuada administración del riesgo, una base confiable para la toma de decisiones y la planificación institucional.

- Establecer lineamientos para la implementación y/o adopción de mejores prácticas de seguridad en la entidad.

- Optimizar la gestión de la seguridad de la información al interior de la entidad.

5. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

El Fondo de Desarrollo de Proyectos de Cundinamarca, mediante la adopción e implementación del Modelo de Seguridad y Privacidad de la Información enmarcado en el Sistema de Gestión de Seguridad de la información, protege, preserva y administra la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información que circula en el mapa de procesos, mediante una gestión integral de riesgos y la implementación de controles físicos y digitales previniendo así incidentes y dando cumplimiento a los requisitos legales y reglamentarios, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información, propendiendo así por el acceso, uso efectivo y apropiación masiva de las TIC.

6. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

El presente documento describe el Plan de Seguridad y Privacidad de la entidad, alineado con los objetivos, metas, procesos, procedimientos y estructura organizacional, de tal forma que se asegure la confidencialidad, integridad y disponibilidad los componentes de información.

Aplica a todos los niveles de Fondecún, a todos sus funcionarios, contratistas, proveedores, operadores y aquellas personas o terceros que en razón del cumplimiento de sus funciones y las de la entidad compartan, utilicen, recolecten, procesen, intercambien o consulten su información.

Así mismo, esta Política aplica a toda la información creada, procesada o utilizada por Fondecún, sin importar el medio, formato o presentación o lugar en el cual se encuentre.

7. METODOLOGIA IMPLEMENTACION MODELO DE SEGURIDAD

El Modelo de Seguridad y Privacidad de la Información de la Estrategia de Gobierno en Línea contempla el siguiente ciclo de operación que contempla cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.

Imagen 1. Ciclo de Operación Modelo de Seguridad y privacidad de la información
Fuente: http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

- 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.
- 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.

8. PLAN DE IMPLEMENTACION

De acuerdo a los resultados del desarrollado en el proceso de la auditoría del MSPI, identificando las brechas existentes, se diseñado un conjunto de actividades orientados a avanzar en diferentes aspectos para dar cumplimiento a las orientaciones del Ministerio de Tecnologías de Información y de las Comunicaciones, en cuanto a la adopción e implementación del modelo de seguridad y privacidad de la información.

No.	Actividad / Plan de mejora	Responsable por parte de la entidad	Fecha de inicio	Fecha de finalización	Producto / entregable
1	Lograr la contratación de un profesional con conocimiento en seguridad informática y en la implementación la Política que permita desarrollar, configurar y ejecutar los controles de los componentes.	Líder gestión tecnológica	15/01/2023	30/03/2023	Desarrollo e implementación de controles de seguridad y componentes del MSPI.
2	Realizar la definición de roles y responsabilidades para la seguridad de la información.	Líder gestión tecnológica	15/01/2023	30/03/2023	Procedimiento revisado y aprobado.
3	Ajustar el procedimiento que especifique cuándo y a través de que autoridades se debe contactar a las autoridades, y cómo se debe reportar de una manera oportuna los incidentes de seguridad de la información identificados (por ejemplo, si se sospecha una violación de la ley).	Líder gestión tecnológica	01/02/2023	30/03/2023	Acta de procedimiento revisado y aprobado.
4	Establecer procedimiento para la revisión de antecedentes de los candidatos a un empleo.	Líder de Talento Humano Líder Oficina Jurídica Área de planeación	01/02/2023	30/07/2023	Acta de aprobación del procedimiento
5	Realizar los soportes documentales que permitan tener resultados de seguimiento, evaluación y análisis al cumplimiento de la seguridad de la información, para cada uno de los planes	Líder gestión tecnológica	15/02/2023	30/12/2023	Soportes de ejecución de actividades de seguridad de la información
6	Desarrollar las guías de Min Tic: Guía 8: Controles de seguridad.	Líder gestión tecnológica	01/03/2023	30/08/2023	Actas de aprobación de los controles de seguridad.
7	Realizar Plan de Recuperación de Desastres	Líder gestión tecnológica	01/03/2023	30/06/2023	Acta de aprobación del plan de recuperación de desastres
8	Realizar el análisis BIA	Líder gestión tecnológica	01/04/2023	30/08/2023	Acta de aprobación de resultados del análisis BIA

9	Terminar la implementación del protocolo IPv6	Líder gestión tecnológica	05/01/2023	30/06/2023	Documentación de la implementación y pruebas
10	Ejecutar plan de capacitación y sensibilización de seguridad	Líder gestión tecnológica	01/03/2023	30/12/2023	Registro de sensibilización realizadas
11	Ejecutar pruebas anuales de vulnerabilidades.	Líder gestión tecnológica	01/06/2023	30/10/2023	Resultado pruebas realizadas.

9. 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.

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.

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. 20

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.

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

10. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS		
VERSIÓN	**FECHA**	**DESCRIPCIÓN DE LA MODIFICACION**
01	**Enero 2021**	**Generación del documento**
02	**ENERO 2022**	**Actualización del documento para la vigencia 2022.**

03	**ENERO 2023**	**Actualización del documento para la vigencia 2023.**

Elaboró y consolidó: Nelson Reina- Profesional con funciones de Gestión tecnológica y de la información