PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

TABLA DE CONTENIDO

Contáctenos
Av-cra 10 # 28-49 Torre A, Piso 21
(57) 1 - 2432328- 2432806
@fondecunoficial
www.fondecun.gov.co

Contáctenos
Av-cra 10 # 28-49 Torre A, Piso 21
(57) 1 - 2432328- 2432806
@fondecunoficial
www.fondecun.gov.co

1. INTRODUCCIÓN

En virtud de la normatividad y las disposiciones legales vigentes en relación con la privacidad y seguridad de la información, y teniendo en cuenta que la información administrativa y misional del Fondo de Desarrollo de Proyectos de Cundinamarca comprende uno de los activos más valiosos y primordiales de la institución cuya integridad asegura el desarrollo de los procesos y procedimientos internos, y el cumplimiento de los objetivos y deberes a cargo de la Entidad, se adopta el Modelo de Seguridad y Privacidad de la Información MSPI en el marco de la política de Gobierno Digital y siguiendo las recomendaciones y directrices expedidas por el Ministerio de Tecnologías de información y de las Comunicaciones, que orientan la política hacia la promoción del uso y aprovechamiento de las tecnologías de la información para consolidar un estado y ciudadanos competitivos, proactivos e innovadores, que generen valor público en un entorno de confianza digital. 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.

De conformidad con lo anterior, 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 establece el presente Plan de Seguridad y Privacidad de la Información el cual 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 colombiano, y de los servicios que se prestan al ciudadano, en concordancia con el ámbito de aplicación del modelo Integrado de Planeación y Gestión. Así, teniendo en cuenta la finalidad del presente plan y su relevancia en la gestión y operación institucional, se lleva a cabo la actualización continua del presente documento en cumplimiento de las disposiciones establecidas mediante Decreto 612 de 2018 "*Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado*".

2. NORMATIVIDAD Y MARCO LEGAL

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

NORMA	ALCANCE
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

Contáctenos
Av-cra 10 # 28-49 Torre A, Piso 21
(57) 1 - 2432328- 2432806
@fondecunoficial
www.fondecun.gov.co

NORMA	ALCANCE
Manual Gobierno en Línea	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.
Ley 1915 de 2018	Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
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 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.
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 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581de 2012.
Resolución 460 de 2022 - Ministerio de Tecnologías de la Información y las Comunicaciones	Por la cual se expide el Plan Nacional de Infraestructura de Datos y Su hoja de ruta en el desarrollo de la Política de Gobierno Digital, y se dictan los lineamientos generales para su implementación.
Resolución 746 de 2022 - Ministerio de Tecnologías de la Información y las Comunicaciones.	Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamentos adicionales a los establecidos en la Resolución No. 500 de 2021.
Constitución Política de Colombia – 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

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

Contáctenos
Av-cra 10 # 28-49 Torre A, Piso 21
(57) 1 - 2432328- 2432806
@fondecunoficial
www.fondecun.gov.co
Gobernación de Cundinamarca

de seguridad de la estrategia de gobierno en línea, los requerimientos del negocio, desde el enfoque de la seguridad informática frente a ciber amenazas.

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. METODOLOGÍA IMPLEMENTACIÓN 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.

Ciclo de Operación Modelo de Seguridad y privacidad de la información[1]

[1] https://gobiernodigital.mintic.gov.co/692/articles-150517_Modelo_de_Seguridad_Privacidad.pdf

Contáctenos
Av-cra 10 # 28-49 Torre A, Piso 21
(57) 1 - 2432328- 2432806
@fondecunoficial
www.fondecun.gov.co

- **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 IMPLEMENTACIÓN

El Fondo de Desarrollo de Proyectos de Cundinamarca adopta el Modelo de Seguridad y Privacidad de la Información teniendo en cuenta los componentes y dominios asociados a la gestión de activos, cifrado, seguridad de las operaciones, seguridad de las comunicaciones, gestión de incidentes y continuidad del negocio, en el marco de un plan de implementación lógico basado en etapas bajo el principio del mejoramiento continuo (PHVA: Planear, Hacer, Verificar y Actuar). Sobre la base de esta premisa de implementación, la Entidad establece el portafolios de actividades y proyectos para el fortalecimiento de las capacidades institucionales en seguridad y privacidad de la información de conformidad con la gestión de la estrategia instruccional que incluye: gestión de riesgos de seguridad, gestión de incidentes, gestión de activos de información, gestión del cambio y cultura, y gestión de la continuidad. En concordancia con lo anterior a continuación se detallan las actividades o proyectos que se desarrollarán para fortalecer la seguridad y privacidad de la información actual de Fondecun.

No.	Actividades/Proyectos		Fecha de [illegible]	Fecha de finalización	Evidencia/Producto	
1	Actualizar el Plan de Tratamientos de Riesgos de Seguridad (gestión de riesgos)	Actualizar los lineamientos de riesgos institucionales	1/01/2025	31/01/2025	Plan de Tratamiento de Riesgos de Seguridad	Esta actividad se desarrollará por una única vez en el año. La evidencia quedará estructurada a más tardar a la fecha de finalización.
		Ejecutar el seguimiento continuo a los controles y planes de tratamiento de riesgos	1/01/2025	31/12/2025	Matriz de estructuración, registro y evaluación de controles	Esta actividad se desarrollará de manera recurrente y se actualizará la matriz correspondiente de forma mensual

Contáctenos
Av-cra 10 # 28-49 Torre A, Piso 21
(57) 1 - 2432328- 2432806
@fondecunoficial
www.fondecun.gov.co

No.	Actividades/Proyectos		Fecha de inicio	Fecha de finalización	Evidencia/Producto	
		Identificar oportunidades de mejora en función de los controles y planes de tratamiento	1/09/2025	31/12/2025	Matriz de estructuración, registro y evaluación de controles	Esta actividad se desarrollará de manera continua durante el último cuatrimestre del año. La matriz se actualizará semanalmente durante tal periodo.
		Identificar riesgos de seguridad digital para los activos de información identificados	1/01/2025	31/12/2025	Matriz de estructuración, registro y evaluación de controles	Esta actividad se desarrollará de manera continua y se actualizará la matriz correspondiente de forma mensual
2	Actualizar el inventario de activos de información (gestión de activos de información)	Actualizar la metodología de identificación y clasificación de activos de información	1/05/2025	31/05/2025	Documento con descripción de la metodología actualizada	Esta actividad se desarrollará en cuatro sesiones de trabajo semanal durante el periodo establecido. En cada sesión se llevará a cabo la actualización del producto
		Validar registros de activos de información de vigencias anteriores	1/06/2025	30/06/2025	Matriz de activos de información registrados	Esta actividad se desarrollará en cuatro sesiones de trabajo semanal durante el periodo establecido. En cada sesión se llevará a cabo la actualización del producto
		Identificar activos de información nuevos en las diferentes áreas o dependencias	1/07/2025	31/08/2025	Matriz de activos de información en construcción	Esta actividad se desarrollará de manera continua durante todo el periodo establecido, y se llevará a cabo la actualización de la matriz correspondiente semanalmente.
		Consolidar y publicar el inventario de activos de información	1/11/2025	30/11/2025	Matriz de activos de información	El producto se actualizará durante el periodo definido para su consolidación a la fecha de finalización.
3	Realizar el seguimiento a la atención de incidentes de TI (gestión de incidentes)	Revisar y actualizar el procedimiento de gestión de incidentes de TI y seguridad	1/05/2025	31/05/2025	Documento con descripción del procedimiento	El documento de procedimiento actualizado se entregará para su aprobación y publicación a la fecha de finalización indicada.
		Llevar a cabo el seguimiento a la atención de los incidentes reportados a la mesa de servicio	1/01/2025	31/12/2025	Registro o reporte en aplicación de gestión de incidentes	Esta actividad se llevará a cabo de forma recurrente y diaria durante el periodo definido.
		Establecer y cuantificar los indicadores de servicio y atención de incidentes	1/10/2025	30/11/2025	Matriz de evaluación y cuantificación de indicadores	En sesiones de trabajo semanal durante el mes de octubre se establecerán los indicadores de servicio de conformidad con los datos y métricas que se registren en la aplicación de mesa de ayuda, y a lo largo del mes de noviembre se cuantificarán tales indicadores.
4	Realizar sensibilización y capacitación a todos los colaboradores de la Entidad sobre los procedimientos de gestión de TI y planes (gestión del cambio y cultura)		1/03/2025	30/09/2025	Informe de capacitaciones	Se llevarán a cabo dos sesiones de sensibilización y capacitación. La primera sesión se desarrollará en el mes de marzo y la segunda sesión se adelantará en el mes de septiembre

Contáctenos
Av-cra 10 # 28-49 Torre A, Piso 21
(57) 1 - 2432328- 2432806
@fondecunoficial
www.fondecun.gov.co

No.	Actividades/Proyectos		Fecha de inicio	Fecha de finalización	Evidencia/Producto	
5	Actualizar, validar y evaluar la eficacia del plan de recuperación de desastres gestión de la continuidad)	Revisar y actualizar el Plan de Recuperación de Destres de ser necesario	1/08/2025	31/08/2025	Documento con descripción del Plan de Recuperaciones de Desastres	A lo largo del mes de agosto se ejecutará esta actividad y se entregará el producto para su aprobación y publicación, en caso de que se actualice, a la fecha de finalización indicada.
		Realizar pruebas de restablecimiento de información desde las copias de seguridad para asegurar la disponibilidad de los datos en caso de incidentes	1/04/2025	31/12/2025	Informe con resultados de las pruebas ejecutadas	Se ejecutarán dos pruebas de restablecimiento de información. La primera prueba se desarrollará en el mes de abril y la segunda prueba en el mes de diciembre. Por cada prueba se elaborará el informe correspondiente el cual quedará finalizado el último día de cada mes señalado.
		Llevar a cabo el diagnóstico de la infraestructura de cómputo y seguridad que soporta los activos de información esenciales, e identificar las oportunidades de mejora y fortalecimiento	1/09/2025	31/12/2025	Informe de diagnóstico y recomendaciones	Esta actividad se desarrollará diariamente durante el periodo definido, y el informe correspondiente quedará estructurado a la fecha de finalización indicada.

Nota: El Líder de Gestión Tecnológica de Fondecun quedará a cargo del desarrollo de las actividades establecidas y de la elaboración, estructuración y consolidación de las evidencias o productos.

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.
- ✓ 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.

Contáctenos
Av-cra 10 # 28-49 Torre A, Piso 21
(57) 1 - 2432328- 2432806
@fondecunoficial
www.fondecun.gov.co
Gobernación de Cundinamarca

- ✓ 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.
- ✓ 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 MODIFICACIÓN**
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.
04	Enero 2024	Actualización de actividades a desarrollar en la vigencia 2024
05	Enero 2025	Actualización de actividades a desarrollar en la vigencia 2024

Contáctenos
Av-cra 10 # 28-49 Torre A, Piso 21
(57) 1 - 2432328- 2432806
@fondecunoficial
www.fondecun.gov.co
Gobernación de Cundinamarca