

**RESOLUCIÓN No. 045 de 2020**  
(30 de diciembre de 2020)

**POR LA CUAL SE ADOPTA LA POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL FONDO DE DESARROLLO DE PROYECTOS DE CUNDINAMARCA – FONDECÚN.**

---

**EL GERENTE GENERAL DEL FONDO DE DESARROLLO DE PROYECTOS DE CUNDINAMARCA - FONDECÚN – FONDECÚN**

En uso de sus atribuciones legales y estatutarias, en especial las conferidas en el artículo 18, numeral 18 y el artículo 19 del Decreto Ordenanza No. 431 de 2020 y

**CONSIDERANDO**

Que en el artículo 15 de la Constitución Política, consagra el derecho fundamental de las personas a conservar su intimidad personal y familiar, al buen nombre y a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellos en bancos de datos y en archivos de las entidades públicas y privadas.

Que la Ley 1273 de 2009 *‘por medio del cual se modifica el Código Penal, 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 “TIC”, entre otras disposiciones’* estableció como conductas punibles agresiones contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, atentados informáticos y otras infracciones.

Que el Decreto 1499 de 2011, el cual modificó el Decreto 1083 de 2015 (Decreto Único Reglamentario del Sector de Función Pública), adoptó el Modelo Integrado de Planeación y Gestión MIPG, definiendo en su artículo 2.2.22.3.2 como *“... un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atienden los planes de desarrollo y resuelvan necesidades y problemas de los ciudadanos, con integridad, y calidad de servicio”*.

Que la ley Estatutaria 1581 de 2012 *“Por la cual se dictan disposiciones generales para la protección de datos personales”*, la cual constituye el marco general de la Protección de Datos Personales en Colombia reglamentando el ejercicio del derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías fundamentales plasmados en los artículos 17, 15 y 20 de la Constitución Política.

Que con el fin de facilitar la implementación y cumplimiento de la Ley 1581 de 2012 en la entidad se deben reglamentar aspectos relacionados con la autorización del Titular de información para el tratamiento de sus datos personales, las políticas de Tratamiento de los Responsables y Encargados,

**RESOLUCIÓN No. 045 de 2020**  
(30 de diciembre de 2020)

**POR LA CUAL SE ADOPTA LA POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA  
INFORMACIÓN DEL FONDO DE DESARROLLO DE PROYECTOS DE CUNDINAMARCA –  
FONDECÚN.**

el ejercicio de los derechos de los Titulares de información, las transferencias de datos personales y la responsabilidad demostrada frente al Tratamiento de datos personales.

Que la ley 1712 de 2014 *"Por medio de la cual se cree la Ley de Transparencia y del Derecho de Acceso a la Información Pública nacional y se dictan otras disposiciones"*, tiene como objetivo principal regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información.

Que el Decreto 1078 de 2015, modificado por 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"*, en el artículo 2.2.9.1.1.3., incluye la seguridad de la información entre los principios de la Política de Gobierno Digital que debe ser aplicado por todas las entidades públicas; de igual manera, en el artículo 2.2.9.1.2.1. se establece que la Política de Gobierno Digital se desarrollara a través de componentes y habilitadores transversales, y respecto de estos últimos indica que son los elementos fundamentales de: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales los que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la política de Gobierno Digital.

Que las entidades que conforman la Administración Pública en los términos del artículo 39 de la Ley 489 de 1998, como el caso del Fondo de Desarrollo de Proyectos de Cundinamarca - Fondecún - Fondecún, están obligados a adoptar la Política de Gobierno Digital, siguiendo los lineamientos del Manual de Gobierno digital, que define procedimientos, estándares y acciones a ejecutar por parte de las entidades.

Que la adopción de un Sistema de Gestión de Seguridad de la Información es una decisión estratégica para una organización. El establecimiento e implementación del sistema de gestión de la seguridad de la información de una entidad pública como es el Fondo de Desarrollo de Proyectos de Cundinamarca - Fondecún, está determinado por las necesidades y objetivos de la entidad, los requisitos de seguridad, los procesos organizacionales empleados, el tamaño y estructura de la organización.

Que conforme a la normatividad citada surge la necesidad de adoptar una política institucional de seguridad y privacidad de la información considerando el papel estratégico de las tecnologías de información y comunicaciones - TIC; así como las herramientas para respaldar las actividades ejecutadas en el Fondo de Desarrollo de Proyectos de Cundinamarca - Fondecún, incentivando la cultura de seguridad de la información a los usuarios, previniendo o solucionando posibles ataques informáticos, virus, robos, uso indebido de software o pérdidas de información.

**RESOLUCIÓN No. 045 de 2020**  
(30 de diciembre de 2020)

**POR LA CUAL SE ADOPTA LA POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA  
INFORMACIÓN DEL FONDO DE DESARROLLO DE PROYECTOS DE CUNDINAMARCA –  
FONDECÚN.**

Que, dado lo anterior se hace necesario adoptar mediante el presente acto administrativo, la Política General de Seguridad y Privacidad de la Información, implementación del Modelo de Seguridad y Privacidad de la Información (MSP), así como definir los lineamientos frente al uso y manejo de la información del Fondo de Desarrollo de Proyectos de Cundinamarca - Fondecún.

En mérito de lo anteriormente expuesto,

**RESUELVE:**

**ARTÍCULO PRIMERO: ADOPTAR** la Política General de Seguridad y Privacidad de la Información y la Política de Tratamiento de datos personales, del Fondo de Desarrollo de Proyectos de Cundinamarca - Fondecún, que hacen parte integral de la presente resolución, y las cuales fueron aprobadas por el comité Institucional de Gestión y Desempeño según acta nro. 4 de fecha 26 de octubre de 2020.

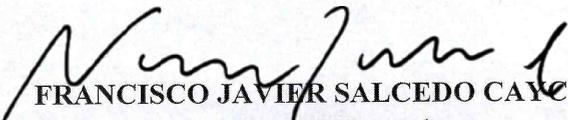
**ARTÍCULO SEGUNDO: ORDENAR** la divulgación de esta política a todas las dependencias del Fondo de Desarrollo de Proyectos de Cundinamarca y publicación en todos los medios de la entidad.

**ARTÍCULO TERCERO. ORDENAR** a la Subgerencia Administrativa y Financiera realizar el seguimiento anual al cumplimiento de la política.

**ARTÍCULO CUARTO.** La presente Resolución rige a partir de la fecha de su expedición, es de obligatorio conocimiento, aplicación y acato por parte de todos los servidores públicos y contratistas de la entidad y deroga todas las disposiciones que le sean contrarias. Contra la misma no procede recurso alguno.

Dado en Bogotá, D.C., a los treinta (30) días del mes de diciembre de 2020.

**PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE**

  
**FRANCISCO JAVIER SALCEDO CAYCEDO**  
Gerente General

V°B°: German Medina Franco – Jefe de Oficina Asesora Jurídica  
Revisó: Ángela Andrea Forero Mojica – Subgerente Administrativa y financiera  
Zayra Daniela Casas Lozano – Profesional Jurídico  
Elaboró: Nelson Andrés Reina Cruz – Contratista

POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

FONDO DE DESARROLLO DE PROYECTOS DE CUNDINAMARCA

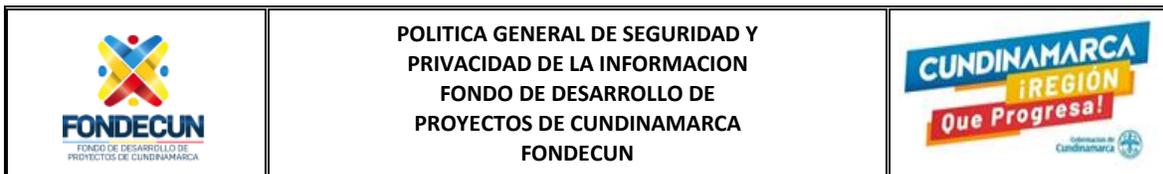
FONDECÚN



**FONDECUN**

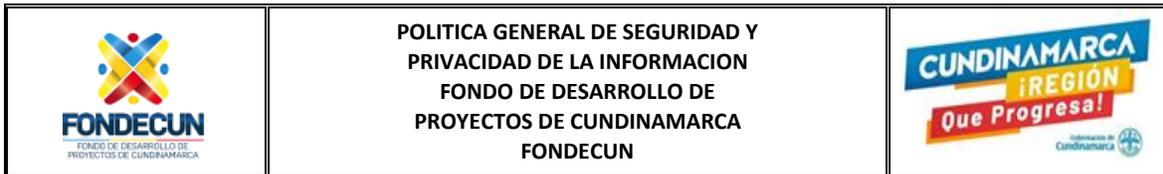
FONDO DE DESARROLLO DE  
PROYECTOS DE CUNDINAMARCA





## CONTENIDO

<b>INTRODUCCION .....</b>	<b>3</b>
<b>1. OBJETIVOS.....</b>	<b>4</b>
<b>1.1 Objetivo General.....</b>	<b>4</b>
<b>1.2 OBJETIVOS ESPECIFICOS .....</b>	<b>4</b>
<b>2. ALCANCE.....</b>	<b>4</b>
<b>3. Definiciones.....</b>	<b>4</b>
<b>4. Política General De Seguridad De La Información .....</b>	<b>6</b>
<b>5. RESPONSABILIDADES .....</b>	<b>8</b>
<b>5.1. Responsabilidades Directivos y Alta Gerencia .....</b>	<b>8</b>
<b>5.2. Responsabilidades Equipo De Gestión .....</b>	<b>8</b>
<b>5.3. Responsabilidades área de tecnologías de la información .....</b>	<b>9</b>
<b>6. Nivel de cumplimiento.....</b>	<b>10</b>
<b>7. ENTRADA EN VIGENCIA .....</b>	<b>10</b>
<b>8. REVISIÓN O ACTUALIZACIÓN DE LA POLÍTICA.....</b>	<b>10</b>



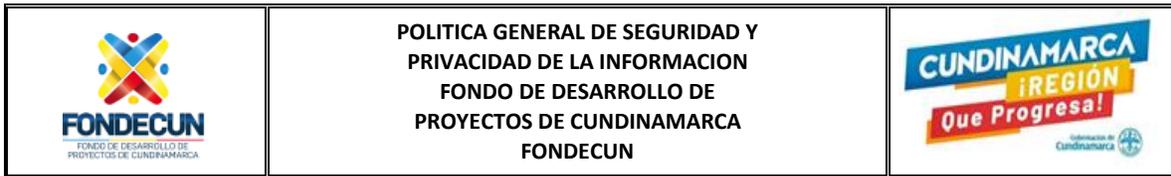
## INTRODUCCION

Las políticas y estándares de seguridad informática establecidas en el presente documento son la base fundamental para la protección de los activos informáticos y de toda la información de las Tecnologías de Información y Comunicaciones (TIC's) en Fondecún.

Según el decreto 1078 de 2015, decreto único reglamentario del sector de tecnologías de la información y las comunicaciones, en la estrategia de gobierno en línea Artículo 2.2.9.1.2,1. Numeral 4, componente de seguridad y privacidad de la información comprende las acciones transversales a los demás componentes, tendientes a proteger la información y los sistemas de información, del acceso, uso, divulgación, interrupción o destrucción no autorizada, y el decreto 1499 decreto único reglamentario del sector Función Pública, en lo relacionado con el Sistema de Gestión el cual se articula con el sistema de seguridad de la información y más aún la seguridad digital, el Fondo de Desarrollo de Proyectos de Cundinamarca – Fondecún, de acuerdo con el Modelo de Seguridad y Protección de la Información, desarrolla e implementa la política general de seguridad de la información, adoptando las políticas necesarias para la protección de la información preservando con calidad, confiabilidad, privacidad, integridad, disponibilidad, y confidencialidad, buscando concientizar a todos los funcionarios y contratistas de la entidad de la importancia del cumplimiento de las normas establecidas y que se aplica a todos los recursos y servicios informáticos existentes en Fondecún.

Este documento describe los principios de seguridad que se deben tener en cuenta para el manejo de la información y de recursos tecnológicos de la entidad, es así como complemento a esta política encontraremos el manual de políticas de seguridad donde se encontrara la gestión para usuario final, manejo de contraseñas, políticas de uso de equipos, políticas del uso de red, políticas de uso de cuentas de correo y protección contra virus informáticos.

Ya que para Fondecún, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.



## 1. OBJETIVOS

### 1.1 Objetivo General

Crear directrices que orienten a los usuarios empleados y contratistas de Fondecún, para un uso responsable de los diferentes recursos y servicios informáticos y de telecomunicaciones, asegurando la información de Fondecún en la integridad, no repudio, disponibilidad, legalidad, y confidencialidad de la información.

### 1.2 OBJETIVOS ESPECIFICOS

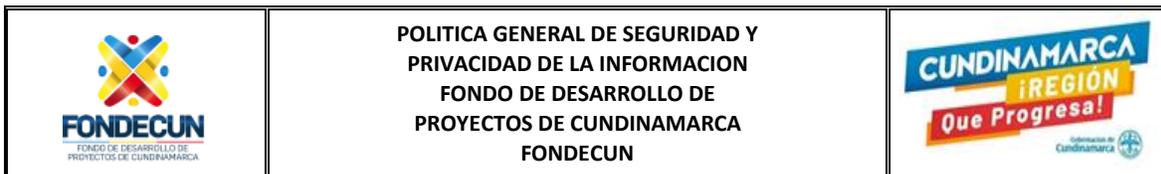
- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de Fondecún.
- Garantizar la continuidad del negocio frente a incidentes.
- Definir lineamientos para el desarrollo de trabajo remoto.
- Fondecún ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

## 2. ALCANCE

Aplica a todos los usuarios que hagan uso de recursos y servicios informáticos y de telecomunicaciones de la infraestructura de Fondecún. De acuerdo con lo anterior, esta política aplica a funcionarios, contratistas, terceros, aprendices, practicantes, proveedores y la ciudadanía en general.

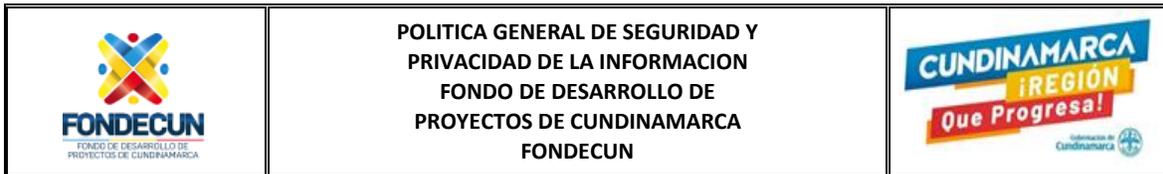
## 3. Definiciones

- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC



27000).

- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- **Autorización:** Consentimiento previo, expreso e informado para llevar a cabo el acceso, manipulación, divulgación o destrucción de la información.
- **Base de Datos:** Conjunto organizado de Datos que sea objeto de tratamiento.
- **Confidencial:** significa que la información no esté disponible o revelada a individuos, entidades o procesos no autorizados.
- **Confidencialidad:** Garantizar que la información es accesible sólo para aquellos autorizados a tener acceso.
- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Hardware:** Conjunto de los componentes físicos que componen la estructura de una computadora.
- **Información pública:** Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.
- **Internet:** Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación.
- **Password:** Una contraseña o password es una serie secreta de caracteres que permite a un usuario tener acceso a un archivo, a un ordenador, o a un programa.
- **Riesgo** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **SGSI:** Sistema de Gestión de Seguridad de la Información



- **Seguridad de la información:** es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información y de los sistemas de información, busca la protección de acceso, de utilización, divulgación o destrucción no autorizada, manteniendo la confidencialidad, la disponibilidad e integridad de datos y de la misma.
- **Trazabilidad** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).
- **Vulnerabilidad** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

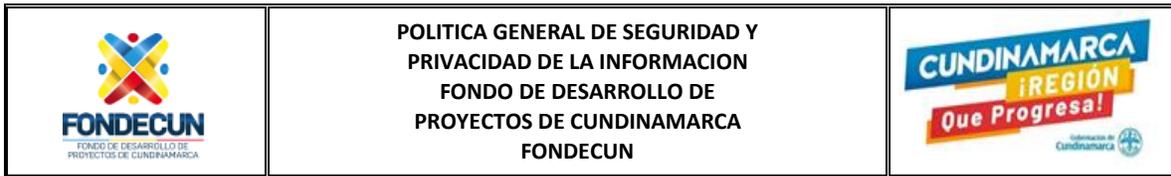
#### 4. Política General De Seguridad De La Información

EL Fondo de Desarrollo de Proyectos de Cundinamarca -Fondecún, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido 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 Fondecún, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

Teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de

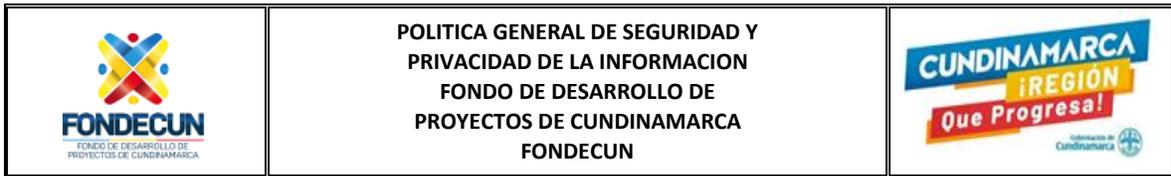


la información.

- Establecer las políticas y procedimientos para la realización de trabajo remoto por parte de los funcionarios y contratistas.
- Fortalecer la cultura de seguridad de la información en los funcionarios, contratistas y clientes de Fondecún.
- Garantizar la continuidad del negocio frente a incidentes.

A continuación se establecen las 12 políticas de seguridad que soportan el SGSI de Fondecún:

1. El Fondo de Desarrollo de Proyectos de Cundinamarca ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.
2. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
3. El Fondo de Desarrollo de Proyectos de Cundinamarca protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.
4. El Fondo de Desarrollo de Proyectos de Cundinamarca protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
5. El Fondo de Desarrollo de Proyectos de Cundinamarca protegerá la información de las amenazas originadas por parte del personal.
6. El Fondo de Desarrollo de Proyectos de Cundinamarca protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
7. El Fondo de Desarrollo de Proyectos de Cundinamarca controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.



8. El Fondo de Desarrollo de Proyectos de Cundinamarca implementará control de acceso a la información, sistemas y recursos de red.
9. El Fondo de Desarrollo de Proyectos de Cundinamarca garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
10. El Fondo de Desarrollo de Proyectos de Cundinamarca garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
11. El Fondo de Desarrollo de Proyectos de Cundinamarca garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
12. El Fondo de Desarrollo de Proyectos de Cundinamarca dispondrá de los procesos adecuados para la realización de trabajo remoto Home Office.
13. El Fondo de Desarrollo de Proyectos de Cundinamarca garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

Las responsabilidades frente a la seguridad de la información del Fondecún son definidas, compartidas, publicadas y deberán ser aceptadas por cada uno de los funcionarios, contratistas o practicantes de Fondecún.

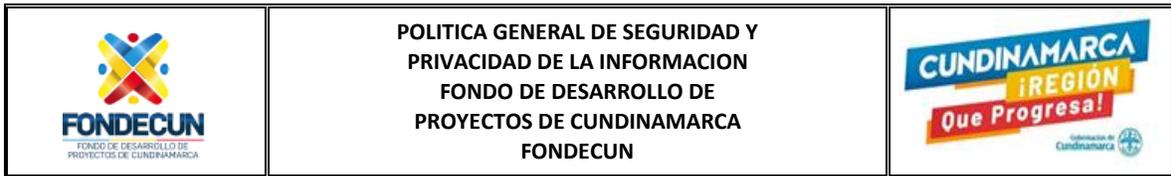
## **5. RESPONSABILIDADES**

La definición de roles y responsabilidades definirá las tareas y procesos a cargo de cada uno de los miembros que conforman dentro de la entidad el modelo de seguridad, permitiendo el desarrollo, adopción e implementación del modelo en la entidad. El organigrama y la definición de roles y responsabilidades se encuentran adicionalmente en el anexo 1 Organigrama.

### **5.1. Responsabilidades Directivos y Alta Gerencia**

Liderar la implementación del modelo de seguridad de la información.  
Definir el grupo responsable que implementara el modelo de seguridad de la información.

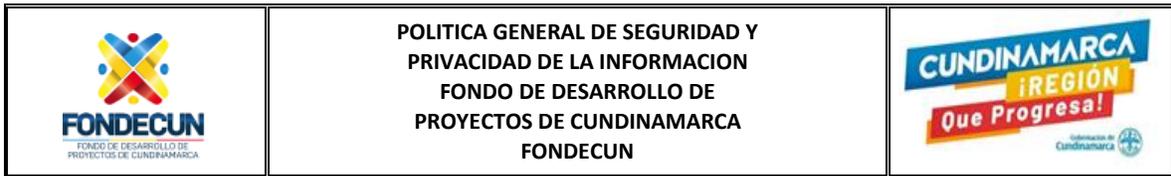
### **5.2. Responsabilidades Equipo De Gestión**



- El equipo de gestión será el encargado de implementar el modelo de seguridad de la información, definiendo e implementando la política.
- Generar el cronograma de la implementación del Modelo de Seguridad y privacidad de la información.
- El equipo de gestión liderara y realizara seguimiento a todas las actividades necesarias para adoptar el Modelo de Seguridad de la Información.
- Planear las actividades necesarias para una adecuada administración y sostenibilidad del mismo.
- Establecer los requerimientos mínimos de seguridad que deberán cumplir los sistemas de información a desarrollar, actualizar o adquirir dentro de la entidad.
- Planear, implementar y hacer seguimiento a las tareas, fechas, costos y plan de trabajo de los objetivos específicos del cronograma definido.
- Realizar un seguimiento permanente a la ejecución de los planes de trabajo, monitoreando los riesgos del proyecto para darle solución oportuna y escalar al Comité de seguridad en caso de ser necesario.
- Monitorear el estado del proyecto en términos de calidad de los productos, tiempo y los costos.
- Liderar la programación de reuniones de seguimiento y velar por la actualización de los indicadores de gestión del proyecto.

### **5.3. Responsabilidades área de tecnologías de la información**

- Instaurar, configurar y publicar la política de seguridad de la información y de todos los servicios tecnológicos a todos los usuarios en la entidad.
- Revisar el cumplimiento de la política de seguridad de la información.
- Salvaguardar la información que reposa en los diferentes sistemas de información, bases de datos y aplicativos de la entidad.
- Evaluar todos los servicios tecnológicos en busca de posibles vulnerabilidades de seguridad de la información.



- Evaluar y realizar junto con el equipo de gestión las correcciones de la política de seguridad Continuamente.
- Proporcionar medidas de seguridad físicas, lógicas y procedimentales para la protección de la información digital de la entidad.
- Analizar, aplicar y mantener los controles de seguridad implementados para asegurar los datos e información gestionados en la Institución.

#### **6. Nivel de cumplimiento**

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

#### **7. ENTRADA EN VIGENCIA**

La presente Política de Seguridad Informática entra en vigencia a partir de la fecha de aprobación por parte de la Gerencia General de Fondecún.

#### **8. REVISIÓN O ACTUALIZACIÓN DE LA POLÍTICA**

La presente política deberá ser revisada con el fin de mantenerla actualizada con los requerimientos de la entidad y de ley una vez cada doce meses como mínimo.