MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN GOBERNACIÓN DE CUNDINAMARCA

TABLA DE CONTENIDO

INTRODUCCIÓN

El manual de políticas de seguridad de la información de la Gobernación de Cundinamarca establece, por una parte, los requisitos fundamentales para preservar la confidencialidad, integridad y disponibilidad de la información, y por otra, determina los procesos, procedimientos y controles que se deben aplicar conforme a la legislación colombiana y a las necesidades y objetivos estratégicos de la Gobernación de Cundinamarca.

Para lograr este objetivo, las políticas aquí definidas brindan las herramientas necesarias para que los funcionarios, contratistas y terceros que hacen parte del Sistema de Gestión de Seguridad de la Información (SGSI en adelante) de la Gobernación de Cundinamarca, puedan adoptar los controles requeridos para asegurar la información, gestionar con eficiencia los riesgos de seguridad y mejorar continuamente el SGSI.

En la actual y cambiante sociedad de la información, toda entidad pública o privada debe lograr una adecuada articulación entre el SGSI y las políticas de seguridad de la información, ello solo es posible a través de la integración de políticas, procedimientos, sistemas de información y controles con un fin común: gestionar de manera pertinente y eficaz los riesgos, de tal forma que las partes interesadas obtengan un alto nivel de seguridad y confianza.

Se entiende, por lo tanto, que las políticas deben ser plenamente conocidas y cumplidas por los funcionarios, contratistas y terceras partes que tienen acceso a los activos de información y a los sistemas de procesamiento de información de la Gobernación de Cundinamarca. En este sentido, es indispensable que sus esfuerzos y capacidades se concentren en lograr los fines primordiales de las políticas, como son: generar controles para proteger los activos de información; crear conciencia en los usuarios acerca del uso responsable de las tecnologías de la información y comunicaciones y realizar una gestión de riesgos adecuada que permita minimizar el impacto frente a un eventual caso de materialización.

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

El objetivo que la Gobernación de Cundinamarca busca con la implementación de su SGSI es mejorar los niveles de seguridad de la información y la protección de los activos de información, para lograrlo sabe que es indispensable implementar los controles según lo señalado por el estándar ISO 27001:2013 y la normatividad vigente aplicable.

Por tal razón, los funcionarios, contratistas y terceros que interactúen con los activos de información de la Gobernación, como ya se ha mencionado, deberán conocer y cumplir las políticas, procesos y procedimientos que hacen parte del SGSI, salvaguardando ante todo los principios de confidencialidad, integridad y disponibilidad que los protegen frente a cualquier tipo de tratamiento.

El SGSI se define para los procesos de Gestión de la Tecnología y Gestión de Talento Humano en la sede de la Gobernación de Cundinamarca, ubicada en Bogotá, en la Calle 26 No 51-53.

2. OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

Los objetivos de seguridad de la información de la Gobernación de Cundinamarca serán aprobados, comunicados y actualizados con base en los siguientes propósitos sustanciales:

- Fortalecer la seguridad de la información, además de promover y mantener la confianza de los funcionarios, contratistas y terceros, mediante el desarrollo, implementación y cumplimiento de las políticas y procedimientos establecidos dentro del SGSI.
- Cumplir con los principios de confidencialidad, disponibilidad e integridad de la información, garantizando la protección de los activos de información de la Gobernación de Cundinamarca.
- Apoyar el cumplimiento de los principios de la función administrativa correspondientes a la legalidad, economía, eficacia, contradicción y publicidad, a través de los lineamientos establecidos por el SGSI.
- Incentivar la cultura de la Seguridad de la Información del Gobernación de Cundinamarca, fortaleciendo las buenas prácticas y la conciencia de

los funcionarios, contratistas y terceros.

- Gestionar los riesgos de seguridad de la información con el fin de evitar el impacto en los objetivos estratégicos de la Gobernación de Cundinamarca, en especial, en aquellos que afecten los procesos misionales.
- Garantizar la continuidad del negocio mediante la implementación de planes y controles que sea necesario desarrollar frente a la existencia de incidentes de seguridad de la información.
- Apoyar las innovaciones y proyectos tecnológicos que garanticen los niveles de seguridad de la información previstos por la Gobernación de Cundinamarca.

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, etc.) que tenga valor para la organización.

- **Amenaza:** causa potencial de un incidente no deseado, que pueda provocar daños a un sistema o a la organización.

- **Amenaza informática:** la aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado (Ministerio de Defensa de Colombia).

- **Análisis de riesgos:** proceso que permite comprender la naturaleza del riesgo y determinar su nivel de riesgo.

- **Anonimización del dato:** eliminar o sustituir algunos nombres de personas (físicas o jurídicas); direcciones y demás información de contacto, como números identificativos, apodos o cargo.

- **Autenticación:** provisión de una garantía de que una característica afirmada por una entidad es correcta.

- **Autenticidad:** propiedad de que una entidad es lo que afirma ser. (ISO 27000.es, 2012).

- **Ciberseguridad: c**apacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

- **Ciberespacio:** ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701).

- **Confidencialidad:** propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

- **Control:** comprenden las políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control también es utilizado como sinónimo de salvaguarda o contramedida, es una medida que modifica el riesgo.

- **Custodio de activo de información:** identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la Gobernación de Cundinamarca, que tiene la responsabilidad de administrar y hacer efectivo los controles que el propietario del activo haya definido, con base en los controles de seguridad disponibles en la entidad.

- **Datos abiertos:** son datos primarios o sin procesar puestos a disposición de cualquier ciudadano, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.

- **Datos biométricos:** parámetros físicos únicos de cada persona que comprueban su identidad y se evidencian cuando la persona o una parte de ella interacciona con el sistema (huella digital o voz).

- **Datos personales sensibles:** se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la

pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

- **Dato privado**: es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

- **Dato público:** es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas.

- **Dato semiprivado:** es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.

- **Disco duro**: disco de metal cubierto con una superficie de grabación ferro magnético. Haciendo una analogía con los discos musicales, los lados planos de la placa son la superficie de grabación, el brazo acústico es el brazo de acceso y la púa (aguja) es la cabeza lectora/grabadora. Los discos magnéticos pueden ser grabados, borrados y re-grabados como una cinta de audio.

- **Disponibilidad:** propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

- **DVD:** Disco Versátil (video) Digital. En la actualidad constituye el natural sucesor del CD para la reproducción de sonido e imagen de calidad.

- **Evento de seguridad de la información:** ocurrencia identificada de estado en un sistema de información, servicio o red que indica una posible brecha de seguridad, falla de un control o una condición no identificada que puede ser relevante para la seguridad de la información.

- **Gestión de claves:** son controles que realizan mediante la gestión de claves criptográficas.

- **Gestión de incidentes de seguridad de la información:** procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

- **Gestión de riesgos:** actividades coordinadas para dirigir controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

- ***Habeas data*:** derecho a acceder a la información personal que se encuentre en archivos o bases de datos; implica la posibilidad de ser informado acerca de los datos registrados sobre sí mismo y la facultad de corregirlos.

- **Impacto:** el coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.

- **Incidente de seguridad de la información:** evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

- **Integridad:** la propiedad de salvaguardar la exactitud y complejidad de la información.

- **Inventario de activos:** lista de todos aquellos recursos (físicos, de información, *software*, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos. (ISO 27000.es, 2012)

- **No repudio**: servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido). (ISO-7498-2).

- **Parte interesada (*Stakeholder*):** persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

- **Plan de continuidad del negocio**: plan orientado a permitir la continuidad de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.

- **Plan de tratamiento de riesgos**: documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

- **Proceso**: conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas. (ISO 27000.es, 2012)

- **Propietario de activo de información:** identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información asignados.

- **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 consideraciones. (ISO Guía 73:2002).

- **Responsable del tratamiento:** persona natural o jurídica. Pública o privada. Que por sí misma o en asocio con otros. Decida sobre la base de datos y/o el Tratamiento de los datos.

- **Segregación de tareas:** reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

- **Seguridad de la información: p**reservación de la confidencialidad, integridad y disponibilidad de la información.

- **Sistema de Gestión de Seguridad de la Información (SGSI):** conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos,

procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basando en un enfoque de gestión y de mejora a un individuo o entidad.

- **Titular de la información:** es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de hábeas data y demás derechos y garantías a que se refiere la presente ley.

- **Trazabilidad:** cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociada de modo inequívoco a un individuo o entidad.

- **Vulnerabilidad:** debilidad de un activo o control que pueda ser explotado por una o más amenazas. (ISO 27000.es, 2012).

4. NORMATIVIDAD

El Sistema de Gestión de Seguridad de la Información de la Gobernación de Cundinamarca se ciñe a la normatividad legal vigente colombiana, tal como se describe enseguida.

LEGISLACIÓN	TEMA	REFERENCIA
Ley 527/99	Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos	El mensaje de datos es "*La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos, Internet, el correo electrónico, el telegrama, el télex o el telefax*".
Ley 594/00	Por medio de la cual se dicta la Ley General de Archivo y se dictan otras disposiciones	La presente ley "*tiene por objeto establecer las reglas y principios generales que regulan la función archivística del Estado". Y "comprende a la administración pública en sus diferentes niveles, las entidades privadas que cumplen funciones públicas y los demás organismos regulados por la presente ley*".
La Ley 850/03 establece en su artículo 9º	Principio de Transparencia	"*A fin de garantizar el ejercicio de los derechos, deberes, instrumentos y procedimientos consagrados en esta ley, la gestión del Estado y de las veedurías deberán asegurar el libre acceso de todas las personas a la información y documentación relativa a las actividades de*

		interés colectivo de conformidad con lo dispuesto en esta ley y en las normas vigentes sobre la materia".
Ley 1266/08	Por la cual se dictan 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.	Se regula el manejo de la información para "*todos los datos de información personal registrados en un banco de datos, sean estos administrados por entidades de naturaleza pública o privada*".
Ley 1221 de 2008	Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones	La presente ley tiene por objeto promover y regular el Teletrabajo como un instrumento de generación de empleo y autoempleo mediante la utilización de tecnologías de la información y las telecomunicaciones (TIC).
Ley 1273/09	Por medio de la cual 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.	"*De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos*".
CONPES 3701 de 2011	Lineamientos de política para ciberseguridad y Ciberdefensa	Busca generar lineamientos de política en ciberseguridad y ciberdefensa encaminados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país.
Resolución 2886 de 2012	Por la cual se definen las entidades que harán parte de la Red Nacional de Fomento al Teletrabajo y se dictan otras disposiciones.	Resolución del Ministerio de Trabajo define "*las entidades que harán parte de la Red Nacional de Fomento al Teletrabajo, las actividades que compete desarrollar y su funcionamiento*".
Ley 1581/12	Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales	Hace referencia, en particular, al artículo 15 de la Constitución Nacional, según el cual "*todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución…*".

		La ley tiene por objeto "*desarrollar el 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 constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma"*.
Decreto 884 de 2012	Por medio del cual se reglamenta la Ley 1221 de 2008 y se dictan otras disposiciones.	El propósito de la Ley 1221 de 2008 es promover y regular el teletrabajo como un instrumento de generación de empleo y autoempleo mediante la utilización de tecnologías de la información y las telecomunicaciones.
Decreto 886 de 2014	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, en lo relativo al Registro Nacional de bases de datos.	Serán objeto de inscripción en el Registro Nacional de Bases de Datos, "l*as bases de datos que contengan datos personales cuyo Tratamiento automatizado o manual se realice por personas naturales o jurídicas, de naturaleza pública o privada, en el territorio colombiano o fuera de él, en este último caso, siempre que al Responsable del Tratamiento o al Encargado del Tratamiento le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales. Lo anterior sin perjuicio de las excepciones previstas en el artículo 2° de la Ley 1581 de 2012*".
En el Decreto Nacional 2573 de 2014	Estrategia de Gobierno en Línea de la República de Colombia	El Decreto establece los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones
LEY 1712 DE 2014	Ley de Transparencia y del Derecho de Acceso a la Información Pública	Hace referencia, principalmente, al artículo 74 de la Constitución Nacional en el cual se establece que "*Todas las personas tiene derecho a acceder a los documentos públicos salvo los casos que establezca la ley*". El objeto de la ley es "*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"*.
Decreto 103 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones	El decreto tiene por objeto 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, y constituye el marco general de la protección del ejercicio del derecho de acceso a la información pública en Colombia.

5. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

OBJETIVO

Definir los lineamientos generales para la protección de los activos de información que orientan los procesos de la Gobernación de Cundinamarca, y de igual manera asignar las responsabilidades que los funcionarios, contratistas y terceros deben cumplir para generar los niveles de seguridad y privacidad de la información determinados por la entidad.

ALCANCE

Esta política aplica a todos los funcionarios, contratistas y terceros de la Gobernación de Cundinamarca.

DETALLE

La Gobernación de Cundinamarca debe salvaguardar las características de integridad, disponibilidad y confidencialidad de la seguridad de la información, mediante la adopción de políticas y procedimientos institucionales orientadas al logro de sus objetivos estratégicos, en estricto cumplimiento de las normas vigentes. De este modo, la Gobernación velará por la adecuada gestión de los riesgos, la adopción de buenas prácticas en el uso de los activos de información y la mejora continua de las competencias del talento humano.

La eficiencia de la política de seguridad de la información se construye a través del liderazgo y compromiso de la Alta Dirección y la participación activa de los funcionarios, contratistas y terceros, quienes mancomunadamente deberán alcanzar el nivel de cumplimiento según los lineamientos y requisitos de seguridad de la información determinados aquí, así como el desarrollo de estrategias de mejora continua y gestión oportuna frente a incidentes o eventos de seguridad de la información.

5.1. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

5.1.1. POLÍTICA DE CONTROL DE ACCESO A LA INFORMACIÓN

OBJETIVO

Definir los lineamientos generales para controlar el acceso a la información y activos de información de la Gobernación de Cundinamarca.

ALCANCE

La política aplica a todos los funcionarios, contratistas y terceros que tengan acceso a la información y activos de información de la Gobernación.

DETALLE

Para preservar la confidencialidad, integridad y disponibilidad de los activos de información que sean objeto de acceso o que se encuentren a disposición de los funcionarios o contratistas en razón de su cargo y/o responsabilidades, la Gobernación de Cundinamarca establecerá controles que permitan regular el acceso a los activos de información y la protección de los mismos.

La Gobernación de Cundinamarca llevará a cabo un control de acceso a la información que tendrá en cuenta tanto los aspectos lógicos como físicos que garanticen la trazabilidad de las acciones realizadas, identificando, entre otros datos relevantes alusivos a: persona que accede, actividades ejecutadas, fecha, hora, lugar, cantidad de intentos de acceso, accesos denegados, entre otros datos que permitan determinar la trazabilidad de las acciones.

Una vez se apruebe el acceso a la información, los funcionarios y contratistas deben tener en cuenta las siguientes precauciones: no efectuar modificaciones a la información accedida sin la debida autorización, guardar confidencialidad de la información, no vulnerar los controles de seguridad establecidos, informar las debilidades o eventos de seguridad de la información al Oficial de seguridad o persona delegada.

RESPONSABILIDADES

- Como responsables de la información, los funcionarios, contratistas y terceros de la Gobernación de Cundinamarca deberán administrar y hacer cumplir los lineamientos establecidos en las políticas de seguridad de la información definidas en este manual, con el fin de evitar accesos no autorizados, pérdidas o utilización indebida de los activos de información.

- Los funcionarios, contratistas y terceros de la Gobernación de Cundinamarca tienen como responsabilidad velar por la integridad, confidencialidad y disponibilidad de la información y/o de los sistemas de información para los cuales han sido autorizados, asegurándose que su acceso y uso responda exclusivamente al desarrollo de las labores propias de la Gobernación de Cundinamarca.

- Los responsables de los activos de información llevarán registros de acceso a dichos activos y sistemas, así como las actividades desarrolladas en razón del tratamiento y la naturaleza gubernamental de la entidad. De igual modo, todos los usuarios tendrán un identificador único (ID del usuario) para su uso personal que permita validar los accesos y verificar su buen uso, actividades podrán ser auditadas con el fin de controlar e investigar todo aquello que así lo demande, siempre con el propósito de minimizar el riesgo de la pérdida de integridad o confidencialidad de la información.

- Los accesos tanto físicos como lógicos, asignados a los funcionarios y contratistas, deberán ser desactivados o modificados una vez terminen sus vínculos contractuales con la Gobernación de Cundinamarca.

- El Gobernación de Cundinamarca establecerá controles para restringir accesos a áreas no autorizadas, entre otros, deberá registrar los sistemas intervenidos, los datos de identificación de la persona que accede, el motivo de ingreso, el tiempo empleado para el desarrollo de la actividad, y asimismo, cuidará que un funcionario del Gobernación acompañe a la persona durante su estancia en el área visitada.

5.1.2. POLÍTICAS DE CIFRADO DE INFORMACIÓN

OBJETIVO

Proteger la confidencialidad, autenticidad o integridad de la información de la Gobernación de Cundinamarca a través de controles criptográficos.

ALCANCE

Las políticas de cifrado se aplicarán para garantizar la confidencialidad, integridad y/o autenticidad en el tratamiento de la información de la Gobernación de Cundinamarca, de acuerdo con los niveles de clasificación determinados y los sistemas electrónicos o de almacenamiento utilizados.

DETALLE

La Secretaría de las TIC, con el apoyo del Oficial de Seguridad de la Información o funcionario delegado, será la encargada de definir los mecanismos de cifrado de información más apropiados frente a las necesidades de la Gobernación de Cundinamarca. Dichas necesidades se determinarán con base en el análisis de riesgos y considerando los criterios de confidencialidad, integridad, autenticidad y no repudio en las comunicaciones durante el tratamiento de la información. El uso de herramientas de cifrado será autorizado conforme a los roles o responsabilidades de los funcionarios y contratistas de la Gobernación.

Para establecer el sistema de cifrado, los responsables de la Gobernación tendrán en cuenta la normatividad colombiana vigente frente a la protección de los datos, estándares aplicables y la tecnología existente. Así mismo, se encargarán de realizar la respectiva activación, recepción y distribución de las llaves criptográficas a los usuarios autorizados y velarán porque la llave se encuentre activa en el período de tiempo previsto.

RESPONSABILIDADES

- La autorización del acceso al sistema de información o a las llaves de cifrado, así como su actualización, deberán solicitarse de manera formal al Oficial de Seguridad de la Información o el funcionario delegado, en la medida en que las actividades laborales así lo demanden.

- Las personas autorizadas para el acceso y uso de las llaves criptgráficas deberán velar por la conservación de la disponibilidad, integridad y confidencialidad de las llaves, así como de la información a la cual se le haya aplicado algún proceso de cifrado. De igual modo, la información cifrada o descifrada deberá ser tratada conforme a su nivel de clasificación y su eliminación deberá realizarse a través de un procedimiento de borrado seguro.

- Los responsables del sistema de cifrado y de las llaves criptográficas serán los encargados de establecer los controles para asegurar el sistema y las llaves, y de restringir su acceso a los funcionarios, contratistas y terceros autorizados. Así mismo tendrán una copia de respaldo que será guardada en sitio seguro por la persona delegada para tal función, y quien procederá a facilitarla en caso de que la llave sea requerida.

- Las actividades relacionadas con la administración y eliminación de las llaves criptográficas deberán ser registradas por la persona encargada. Las llaves serán deshabilitadas cuando estas tengan riesgo de divulgación o cuando los funcionarios, contratistas y terceros autorizados culminen su relación laboral o contractual con la Gobernación de Cundinamarca.

- Los funcionarios, contratistas y terceros tendrán la responsabilidad de reportar, mediante los canales autorizados, las fallas reales o potenciales del sistema o los posibles riesgos asociados al cifrado de la información.

5.1.3. POLÍTICA DE TRANSFERENCIA O INTERCAMBIO DE INFORMACIÓN

OBJETIVO

Definir las pautas generales que se deben seguir para preservar sus características de disponibilidad, integridad y confidencialidad de la información durante su intercambio tanto entre los funcionarios, contratistas y terceros de la Gobernación así como con entidades externas.

ALCANCE

La presente política deberá ser adoptada por todos los funcionarios, contratistas y terceros de la Gobernación de Cundinamarca que realicen intercambio de

información en cumplimiento de sus funciones.

DETALLE

El control de la transmisión de la información de la entidad se efectuará según los niveles de clasificación de la información establecidos y las políticas de seguridad de la Gobernación de Cundinamarca. En caso de que se requiera intercambiar información, se deberán adoptar controles de cifrado de información de acuerdo con los niveles de clasificación y los controles determinados por la entidad.

Los intercambios de información con otras entidades o partes interesadas externas deberán formalizarse mediante contratos o acuerdos escritos, determinando en ellos los medios y controles en el tratamiento de la información. Se firmarán de igual modo acuerdos de confidencialidad que garanticen la protección de la información durante y posterior al tiempo de ejecución de las labores encomendadas.

La transmisión de la información se desarrollará de acuerdo con la normatividad colombiana aplicable, en especial, la Ley de *Habeas Data* (Ley 1266 de 2008), la Ley de Protección de Datos Personales (Ley 1581 de 2012 y decretos reglamentarios) y la Ley de Transparencia (Ley 1712 de 2014), que se pueden observar en detalle en el **numeral 3** del presente manual.

Una vez realizado el intercambio de la información, sólo podrá ser usada exclusivamente para las labores establecidas, es decir, no se podrá compartir, reproducir y/o usar sin previa autorización.

RESPONSABILIDADES

- La presente política es de obligatorio cumplimiento por parte de los funcionarios, contratistas y terceros que realizan intercambio de información dentro o fuera de la Gobernación de Cundinamarca. Por esta razón tendrá como precedente que el único propietario de la información es la Gobernación y sólo podrá ser usada para los fines pertinentes y autorizados.

- La información deberá protegerse de divulgación no autorizada conforme lo señalan los Procedimientos de Clasificación y Etiquetado de la Información,

siguiendo los mecanismos y controles establecidos para el tratamiento de la información.

- La información sólo podrá ser usada en las actividades asignadas dentro de los acuerdos suscritos entre de la Gobernación de Cundinamarca y las partes interesadas.

- El intercambio de información se efectuará según los acuerdos establecidos, que tendrán descrito como mínimo: las responsabilidades y procedimientos para la transferencia de información que permita garantizar la trazabilidad y no repudio, el responsable y proceso a seguir en caso de presentarse un incidente de seguridad y los niveles de clasificación de la información a ser intercambiada y tratada por las partes.

- Para la transferencia de información se tendrán presentes los riesgos asociados y los canales utilizados que brinden los niveles de seguridad apropiados. Estos medios serán dispuestos por la Secretaría de las TIC y el Oficial de Seguridad de la Información.

- Se firmarán acuerdos de confidencialidad con las partes interesadas en acceder e intercambiar información perteneciente a la Gobernación de Cundinamarca, en los cuales se registren las responsabilidades y se garanticen la reserva de la información y el alcance frente a su tratamiento.

5.1.4. POLÍTICA DE USO DE DISPOSITIVOS MÓVILES

OBJETIVO

Garantizar la seguridad de la información en los dispositivos móviles cuando se administre, transmita o almacene información de la Gobernación de Cundinamarca.

ALCANCE

La presente política aplica a todos los dispositivos y equipos móviles de los funcionarios, contratistas y terceros de la Gobernación de Cundinamarca que

tengan acceso a la red, a la información o a cualquier servicio de tecnologías de la información y las comunicaciones de la entidad.

DETALLE

La Gobernación de Cundinamarca implementará las directrices necesarias para la autorización de acceso a los recursos y activos de información a través de los dispositivos de tecnología móviles (computadores portátiles, tarjetas inteligentes, teléfonos celulares, entre otros). Así mismo, conforme a los riesgos asociados establecerá mecanismos de control de seguridad de la información de estricto cumplimiento por parte de los funcionarios, contratistas y terceros que accedan desde dichos dispositivos a la información, tecnologías de la información y comunicaciones o servicios y recursos de la Gobernación de Cundinamarca.

CONDICIONES OBLIGATORIAS

- Existirán redes segmentadas con los controles establecidos por la Secretaría de las TIC, para que los funcionarios, contratistas y terceros puedan acceder al recurso, manteniendo la seguridad de los activos de información de la Gobernación de Cundinamarca.

- Se deberán proteger física y lógicamente los dispositivos móviles propiedad de la Gobernación de Cundinamarca con el fin de evitar el hurto, acceso o la divulgación no autorizada de la información. En caso de ser necesario, se cifrará la información y se tendrán copias de respaldo.

- La Secretaría de las TIC, con la información suministrada por el Secretaría de la Función Pública, brindará o denegará a los funcionarios, contratistas y terceros el acceso a la información o sistemas de información a través de los dispositivos móviles conforme los roles y responsabilidades.

- En caso de extravió o hurto de un dispositivo móvil asignado por la Gobernación de Cundinamarca, el funcionario, contratista o tercero será el responsable de informar el hecho de manera inmediata a la entidad y a su vez al Oficial de Seguridad de la Información, con el propósito de establecer de las medidas de seguridad adecuadas y oportunas para la protección de la información contenida.

RESPONSABILIDADES

- Todos los funcionarios, contratistas y terceros que tengan acceso a la información o sistemas de información a través de los dispositivos móviles deberán cumplir la presente política.

- La Secretaría de las TIC establecerá los mecanismos de seguridad adecuados para proteger la información contenida y transmitida desde los dispositivos móviles de los funcionarios, contratistas y terceros de la Gobernación de Cundinamarca.

- El Oficial de Seguridad de la Información junto con el Secretaría de la Función Pública realizarán campañas de sensibilización periódicas a los funcionarios, contratistas y terceros de la Gobernación, con el propósito de concientizar sobre al uso responsable de dispositivos móviles.

5.1.5. POLÍTICA PARA RELACIONES CON PROVEEDORES

OBJETIVO

Preservar los niveles de seguridad y privacidad de los activos de información de la Gobernación de Cundinamarca accedidos o administrados por proveedores, a través de la implementación de controles que minimicen los riesgos asociados.

ALCANCE

La presente política aplica a todos los funcionarios y contratistas de la Gobernación de Cundinamarca que tengan relaciones con proveedores que accedan y operen activos de información de la entidad.

DETALLE

Cuando se requiera otorgar acceso a los activos de información a los proveedores de la Gobernación de Cundinamarca, el responsable del activo, con el apoyo del Oficial de Seguridad, deberá realizar un análisis de riesgos con el fin de determinar los controles de seguridad que preserven la confidencialidad, disponibilidad e integridad, así como la finalidad del uso de los datos y el

respectivo consentimiento en los casos que aplique, conforme a los niveles de clasificación, requerimientos legales y administrativos.

Antes de conceder los permisos de acceso se determinarán por parte del responsable del activo, entre otros aspectos: las necesidades del acceso, tipo de acceso, el nivel de clasificación de la información a acceder, la finalidad de uso, los controles mínimos a tener en cuenta frente al tratamiento de la información y el manejo de incidentes de seguridad de la información. De igual manera, se validarán los antecedentes del proveedor conforme a los procedimientos establecidos por la Gobernación de Cundinamarca, con el objeto de garantizar el adecuado manejo de la información.

Los funcionarios o contratistas en ningún caso otorgará acceso a los activos de información o áreas críticas de la Gobernación a proveedores, hasta no haber gestionado los riesgos, haber formalizado la relación contractual y firmado el acuerdo de confidencialidad.

Dentro de los acuerdos, contratos o convenios formalmente firmados entre las partes se deberán definir claramente los requerimientos de seguridad y privacidad tales como: información a tratar; niveles de clasificación; finalidad; autorizados para el tratamiento; controles a tener en cuenta antes, durante y después del tratamiento de los datos por parte del proveedor, con el respectivo consentimiento de los titulares en los casos que aplique; así como las responsabilidades de las partes conforme a los lineamientos de la Gobernación de Cundinamarca y a la legislación vigente.

Siempre que se otorgue el acceso a los activos de información de la Gobernación de Cundinamarca a proveedores, se establecerán acuerdos de confidencialidad que tengan como principio el cumplimiento de las políticas de seguridad de la información y las cláusulas requeridas para su protección.

RESPONSABILIDADES

- Los funcionarios, contratistas y proveedores que tengan acceso a la información deberán cumplir con la presente política, así mismo, en caso de que identifiquen una amenaza que pueda llegar a vulnerar la información,

deberán reportarla al Oficial de Seguridad a través de los conductos establecidos.

- El Responsable del activo de información no permitirá el acceso a la información hasta no tener firmados y formalizados, mediante un contrato o acuerdo con los proveedores, los fines de uso, condiciones de tratamiento, así como la debida implementación de los controles requeridos para preservar las características de confidencialidad, integridad y disponibilidad de los activos de información.

5.1.6. POLÍTICA DE TELETRABAJO

OBJETIVO

Definir las pautas generales para conservar los niveles de seguridad de los activos de información durante el desarrollo de actividades de teletrabajo.

ALCANCE

La política aquí descrita aplica a todos los funcionarios, contratistas y terceros de la Gobernación de Cundinamarca que hayan sido autorizados para realizar actividades de teletrabajo.

DETALLE

La Gobernación de Cundinamarca autorizará las actividades de teletrabajo según sus necesidades, condiciones del trabajo, roles y perfiles de los funcionarios, contratistas y terceros de la entidad. Las actividades de teletrabajo sólo se podrán desarrollar una vez se establezcan controles de seguridad alineados con las políticas de seguridad de la información de la Gobernación de Cundinamarca y frente al respectivo análisis del riesgo.

La Gobernación de Cundinamarca proveerá mecanismos de seguridad física y lógica a los equipos y documentos requeridos para el desarrollo de las actividades de teletrabajo, con el fin de garantizar las características de integridad, disponibilidad y confidencialidad de la información.

- Antes del desarrollo de las actividades de teletrabajo la Gobernación de Cundinamarca realizará un análisis de riesgos que permita adoptar y adecuar los mecanismos de control indispensables para la protección a sus activos de información.

- Antes de llevar a cabo cualquier actividad de teletrabajo, la Gobernación de Cundinamarca definirá con funcionarios, contratistas y tercer el alcance de las actividades a desarrollar, determinando como mínimo: la información a acceder, el horario, sistemas, activos de información y servicios de la Gobernación de Cundinamarca requeridos para el desarrollo de las actividades.

- En caso de presentarse un incidente o evento de seguridad de la información, se deberá reportar de inmediato, siguiendo el Procedimiento de Gestión de Incidentes de Seguridad para el desarrollo de las actividades a que haya lugar por parte de la Gobernación.

- La Secretaría de las TIC, con la información remitida por el Secretaría de la Función Pública, brindará o denegará el acceso a la información o sistemas de información que puedan ser accedidos a través de los equipos usados para las actividades de teletrabajo.

RESPONSABILIDADES

- Se adoptarán mecanismos de seguridad por la Secretaría de las TIC, con el objeto de proteger la información contenida y transmitida desde los equipos que se vinculen con las actividades de teletrabajo en la Gobernación de Cundinamarca.

- El Oficial de Seguridad de la Información, junto con el Secretaría de la Función Pública, realizará campañas de sensibilización para promover buenas prácticas en las actividades de teletrabajo.

- La Secretaría de las TIC, en coordinación con el Oficial de Seguridad, determinará los canales de comunicación y los métodos de autenticación apropiados para controlar el acceso de usuarios remotos a la información y sistemas de información de la Gobernación.

5.1.7. POLÍTICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA

OBJETIVO

Establecer los lineamientos generales para que los funcionarios, contratistas y terceros de la Gobernación de Cundinamarca conserven el puesto del trabajo y pantalla del equipo de cómputo limpio de documentos, archivos o dispositivos de almacenamiento removibles.

ALCANCE

Los funcionarios, contratistas y terceros de la Gobernación de Cundinamarca que tengan acceso a la información tanto en formato físico como digital deberán cumplir con la política aquí descrita.

DETALLE

El adecuado aseguramiento de la información de la Gobernación de Cundinamarca demanda de los funcionarios, contratistas y terceros la adopción de buenas prácticas en el manejo y administración de la información física y electrónica a su cargo, conforme a su clasificación, con el fin de evitar el acceso a personas no autorizadas. Para ello, deberán tener presente:

- Almacenar de forma segura documentos y elementos de almacenamiento externos (CD, DVD, USB, etc.) en cajones bajo llave, con el fin de evitar accesos no autorizados, pérdida o daño de la información en la jornada laboral o fuera de ella.

- Durante los lapsos de tiempo en los cuales cesan las actividades en las estaciones de trabajo, se tendrá la responsabilidad de bloquear la sesión del equipo para evitar que terceros no autorizados accedan a la información contenida en el computador. Así mismo, se generarán los controles adecuados para los documentos físicos que reposa en el lugar de trabajo.

- Una vez culmine el proceso de impresión o copiado, los documentos deberán ser retirados por el funcionario responsable de forma inmediato.

- Así mismo, conforme los niveles de clasificación de la información, los archivos o carpetas deberán ser almacenados en rutas que impidan el fácil acceso por parte de terceros, evitando, por ejemplo, guardarlos en el escritorio del sistema de cómputo.

RESPONSABILIDADES

- Los funcionarios, contratistas y terceros de la Gobernación de Cundinamarca serán los responsables del buen uso de la información tanto física como lógica, y del cumplimiento de los lineamientos determinados en esta política.

- Los equipos de cómputo y lugares de trabajo podrán ser revisados y auditados por las áreas de control que determine la Gobernación de Cundinamarca, a fin de validar el cumplimiento de la presente política.

- La Secretaría de las TIC, con el apoyo del Oficial de Seguridad, será la encargada de establecer controles de bloqueo sobre las sesiones de los usuarios para que el equipo se bloquee en un lapso de tiempo determinado.

5.1.8. POLÍTICA DE RESPALDO DE INFORMACIÓN

OBJETIVO

Definir los lineamientos generales para la generación, administración y custodia de las copias de respaldo, con el fin de preservar la disponibilidad e integridad de la información.

ALCANCE

Esta política es de obligatorio cumplimiento por parte de los funcionarios, contratistas y terceros que realicen, administren y custodien las copias de respaldo definidas por la Gobernación de Cundinamarca, reduciendo ante todo el impacto frente a la pérdida de información o a incidentes que comprometan la continuidad del negocio.

DETALLE

La información requerida en el desarrollo de las operaciones orientadas al cumplimiento de los objetivos estratégicos de la Gobernación de Cundinamarca, deberá tratarse conforme a los lineamientos legales, técnicos y administrativos determinados conforme a las tablas de retención documental, la gestión de riesgos, así como a los niveles de clasificación de la información.

Los tiempos de preservación de las copias de respaldo de la Gobernación se definirán según los requerimientos técnicos, administrativos y jurídicos, y se determinarán por parte de la entidad los recursos requeridos para acceso y validación de la información contenida durante los tiempos previstos.

La solicitud de respaldo deberá presentarse formalmente al responsable de las copias de respaldo, determinando las necesidades, la información sujeta al respaldo, periodos, niveles de clasificación de la información y el tiempo de retención de las copias. Así mismo, se realizarán las respectivas pruebas de funcionamiento conforme a los propósitos para los cuales han sido recaudadas.

Los funcionarios encargados de las copias de respaldo, velarán para que durante su transporte y custodia, la misma no sea manipulada por personas no autorizadas.

Las copias de respaldo deberán ser almacenadas en lugares que tengan los debidos controles de seguridad físicos y tecnológicos, esto es, que permitan limitar el acceso sólo a las personas autorizadas y garanticen la disponibilidad de la información. A su vez, deberán registrarse todas las actividades desarrolladas frente al tratamiento y manipulación de las copias para guardar la trazabilidad.

Cumplido el tiempo requerido de almacenamiento de las copias de respaldo, se deberá proceder a su destrucción o eliminación, asegurando que la información contenida no sea accedida por personas no autorizadas. Las actividades realizadas deberán ser registradas para su posterior consulta.

RESPONSABILIDADES

- Los funcionarios, contratistas y terceros responsables de la infraestructura, sistemas de información y Bases de datos requeridos para la operación de la Gobernación de Cundinamarca, deberán generar las respectivas copias

de respaldo, estableciendo la periodicidad, tipo de almacenamiento y registrando la información según lo establecido en la presente política.

- Los encargados de las copias de respaldo deben velar porque la información sea almacenada conforme a los lineamientos establecidos, es decir, de forma controlada y según las necesidades de la Gobernación de Cundinamarca. Así mismo deberán realizar una prueba periódica de las copias con el fin validar el correcto funcionamiento y la efectiva restauración.

- Los dueños de los procesos o activos de información, serán los encargados de velera por que las copias se realicen de acuerdo con lo establecido y que las mismas se ajusten a las necesidades y requerimientos, garantizando el cumplimiento de los objetivos estratégicos y misionales de la Gobernación de Cundinamarca.

- Los funcionarios, contratistas y terceros de la Gobernación de Cundinamarca deberán almacenar la información requerida para sus procesos operativos, dentro del servidor de almacenamiento provisto por la Gobernación, con el fin de garantizar la disponibilidad y copias de respaldo de cada una de las áreas. Así mismo serán responsables de depurar la información para la optimización de los recursos.

5.1.9. POLÍTICA DE DESARROLLO DE *SOFTWARE*

OBJETIVO

Definir los lineamientos generales para el desarrollo y adquisición de *software* al interior de la Gobernación de Cundinamarca, con el fin de determinar los controles de seguridad en el desarrollo de código fuente.

ALCANCE

Los funcionarios, contratistas y terceros de la Gobernación de Cundinamarca que realicen actividades relacionadas con el desarrollo de *software* deberán cumplir la presente política.

DETALLE

Para el desarrollo de *software* se deberá realizar un proceso de planeación en el cual se determine la metodología a utilizar; las etapas de desarrollo; la estructura de desglose de trabajo, con sus respectivos responsables; criterios de aceptación y las pruebas de funcionalidad y seguridad, teniendo en cuenta los requerimientos y el cumplimiento de los objetivos estratégicos de la Gobernación de Cundinamarca. Las etapas deberán estar debidamente documentadas, con el objeto de generar registros de trazabilidad frente a los requerimientos, desarrollo y aceptación del *software*.

Los Jefes de las áreas deberán presentar de manera formal la solicitud de desarrollo de *software*. En ella deberán establecer las necesidades y requisitos a satisfacer y cumplir. Con el apoyo de la Secretaría de TIC se determinarán los requisitos de calidad y seguridad que deberán ser validados durante el proceso de aprobación del *software*.

Para el desarrollo y puesta de producción del *software*, se deberá disponer de tres ambientes separados, los cuales corresponden a; desarrollo, pruebas y producción, conformados por infraestructura y personal propios en cada uno de ellos, evitando así las alteraciones o modificaciones no autorizadas al código.

Los cambios requeridos para el desarrollo del *software* de la Gobernación de Cundinamarca se llevarán a cabo a través del Procedimiento de Control de Cambios, el cual permite que se documenten y establezcan los requerimientos y los niveles de aceptación del cambio. Dentro de los requerimientos que se establezcan será necesario analizar los riesgos asociados a la seguridad de la información y los controles para su mitigación.

Se establecerán acuerdos en procesos de desarrollo que establezcan con claridad la propiedad de las licencias y derechos intelectuales de los códigos fuente, así como sus condiciones de usabilidad.

RESPONSABILIDADES

- Antes de iniciar el desarrollo de *software*, la Secretaría de las TIC, el Oficial y las áreas de la Gobernación de Cundinamarca involucradas, deberán acordar una metodología; que determine como mínimo la estructura de

trabajo, responsables, cronograma, alcance, procesos afectados y requerimientos.

- La Secretaría de las TIC, en coordinación con el Oficial de Seguridad, validará los criterios de aceptación de seguridad, requeridos para otorgar la aceptación formal del desarrollo de *software*. La aceptación de los criterios estará determinada por los resultados de las pruebas planteadas, las cuales tendrán dentro de sus objetivos detectar, entre otras vulnerabilidades, los códigos maliciosos, las puertas traseras, etc.

- En el desarrollo de *software* se establecerán controles que permitan conservar la seguridad y privacidad de la información; entre otros, se deberán tener en cuenta los mecanismos de acceso a la información, autenticación, detección de intrusos, cifrado de datos, salvaguarda de confidencialidad, integridad, disponibilidad y protección de los datos personales.

- Realizar un análisis de los riesgos asociados a los nuevos desarrollos que determine los niveles de afectación en caso de materializarse uno de los riesgos y los controles establecidos para mitigarlos y/o aceptarlos.

- La Secretaría de las TIC, en conjunto con el Oficial de Seguridad, deberá llevar a cabo auditorías y revisiones periódicas a los desarrollos realizados, con el propósito de garantizar que se estén desplegando los controles conforme a lo establecido dentro de la fase de planeación.

- La Secretaría de las TIC llevará a cabo el control de versionamiento del *software* desarrollado con los respectivos documentos de soporte, con el objeto de verificar el buen funcionamiento y el respectivo control del ciclo de vida del *software*.

5.1.10. POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

OBJETIVO

Establecer las medidas generales para garantizar los niveles de seguridad y privacidad adecuados para la protección de datos personales, con el propósito de evitar posibles adulteraciones, pérdidas, consultas, usos o accesos no autorizados.

ALCANCE

La presente política será aplicable a los datos personales registrados en cualquier base de datos de la Gobernación de Cundinamarca, cuyo titular sea una persona natural.

DETALLE

La Gobernación de Cundinamarca implementará una política de Tratamiento de la información, en un lenguaje claro y sencillo, que deberá ser puesta en conocimiento de los Titulares y tendrá que incluir como mínimo:

1. Nombre o razón social, domicilio, dirección, correo electrónico y teléfono del Responsable.
2. El Tratamiento al cual serán sometidos los datos y la finalidad del mismo, si este no se ha informado por medio del aviso de privacidad.
3. Derechos que asisten a los Titulares de la información.
4. El área o persona responsable de la atención de las consultas, peticiones y reclamos ante la cual el Titular de la información puede ejercer sus derechos.
5. Procedimiento por medio del cual los titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar, suprimir información y revocar la autorización.

Los mecanismos para la autorización del tratamiento de los datos personales podrán ser determinados a través de medios técnicos, de forma oral o por medio de conductas inequívocas que permitan otorgar la autorización por parte del Titular y los mismos deberán ser conservados por los responsables del tratamiento.

Así mismo, los funcionarios, contratistas o terceros sólo deberán recopilar la cantidad mínima de datos personales requerida para cumplir con los propósitos de la Gobernación de Cundinamarca. Dicho recaudo sólo se realizará una vez se obtenga la respectiva autorización.

Además, el Responsable de las bases de datos deberá adoptar las medidas necesarias para garantizar la seguridad de los datos de carácter personal y así evitar su destrucción, alteración, pérdida o tratamiento no autorizado. Estas medidas deberán incluir los mecanismos de seguridad físicos y lógicos más adecuados, de acuerdo con el desarrollo tecnológico, de tal forma que garanticen la protección de la información almacenada y el secreto profesional.

Las bases de datos que contengan datos personales, deberán ser administradas de tal modo que se garantice el respeto a derechos fundamentales como la intimidad, el buen nombre, y en especial, el *Habeas Data*.

Ningún funcionario o contratista del Gobernación de Cundinamarca deberá retirar o transmitir información que contenga datos personales sin la debida autorización expresa del Responsable; y en caso de que se facilite información a terceros, se deberá garantizar el buen uso y contar con el debido consentimiento para el tratamiento de los datos conforme a su finalidad, firmado por el titular de los datos. Los mecanismos de transferencia se realizarán a través de las políticas y procedimientos de seguridad y privacidad descritas en el presente manual.

Los responsables y encargados del tratamiento de los datos personales sólo podrán recolectar, almacenar, usar o circular los datos durante el tiempo establecido para cumplir las finalidades que justificaron el tratamiento. Por lo tanto, una vez se cumpla con los objetivos y las finalidades del tratamiento, el Responsable y el Encargado deberán suprimir de una forma segura los datos personales que tengan en su posesión.

Los funcionarios, contratistas y terceros de la Gobernación de Cundinamarca no podrán realizar el tratamiento de datos personales de niños, niñas y adolescentes, excepto cuando se trate de datos públicos. En este caso, la Gobernación de Cundinamarca deberá respetar los intereses y los derechos fundamentales, conforme a la autorización previa del representante legal de cualquiera de ellos.

Si no es posible poner a disposición del Titular la información relacionada con las políticas de tratamiento, los responsables deberán informarle por medio de un Aviso de Privacidad sobre su existencia y la forma en la cual puede acceder a ellas, a más tardar en el momento en el que se vaya a realizar la recolección de datos personales.

RESPONSABILIDADES

- Los funcionarios, contratistas y terceros que tengan acceso a datos personales tratados y administrados por la Gobernación de Cundinamarca, deberán cumplir con la política aquí descrita, haciendo uso de los controles y medidas establecidas para la protección de la información conforme a su nivel de clasificación.

- El Responsable de las bases de datos que contengan información personal, deberá asegurar que antes de realizar cualquier tratamiento de los datos, la Gobernación de Cundinamarca cuente con las autorizaciones de los Titulares y los mecanismos de control para la protección de la información.

- Los funcionarios, contratistas y terceros deberán evitar el acceso a los datos personales para los cuales no se encuentren autorizados y en caso de que observen violación o fallas de los mecanismos de control de seguridad y privacidad, deberán ser reportados oportunamente al Oficial de Seguridad para determinar las acciones a desarrollar.

- Toda transferencia de datos personales se deberá realizar según lo establecido en el Procedimiento Transferencia de Información de la Gobernación de Cundinamarca.

- Se deberán actualizar periódicamente las listas de acceso de las personas y funcionarios autorizados para efectuar cualquier tipo de tratamiento de datos personales. Así mismo, se identificarán, de acuerdo con los niveles de clasificación, los mecanismos apropiados para garantizar la seguridad de los datos de carácter personal y evitar su alteración, pérdida, tratamiento o acceso no autorizado.

- Cumplido el lapso de tiempo del tratamiento de los datos personales, el Responsable deberá velar porque sean eliminados de forma segura, y evitar así su recuperación.