Sistema Integrado de Gestión

# PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

**Código: MGTICS - 001**

CARTAGENA DE INDIAS D. T. y C, 14 DE ENERO DE 2026

## 1. INTRODUCCIÓN

El presente Plan de Seguridad y Privacidad de la Información 2026 desarrolla, implementa y operacionaliza lo establecido en el Modelo de Seguridad y Privacidad de la Información (MSPI) adoptado por la entidad, en concordancia con el Decreto 612 de 2018 y los lineamientos del MinTIC

### 1.1 Objeto

Definir los mecanismos y todas las medidas necesarias por parte de Distriseguridad, tanto técnica, lógica, física, legal y ambiental para la protección de los activos de información, los recursos y la tecnología de la entidad, con el propósito de evitar accesos no autorizados, divulgación, duplicación, interrupción de sistemas, modificación, destrucción, pérdida, robo, o mal uso, que se pueda producir de forma intencional o accidental, frente a amenazas internas o externas, asegurando el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

### 1.2 Alcance

Este plan aplica a toda la información en cualquier formato (física, digital, verbal) que sea propiedad de la entidad o esté bajo su custodia, así como a todos los funcionarios, contratistas, proveedores y terceros que tengan acceso a los activos de información.

### 1.3 MARCO NORMATIVO APLICABLE

**Normatividad General:**
Ley 1581 de 2012 - Protección de Datos Personales
Decreto 1377 de 2013 - Reglamenta parcialmente la Ley 1581
Ley 1712 de 2014 - Ley de Transparencia y Acceso a la Información Pública
Ley 1273 de 2009 - Delitos Informáticos
Decreto 1083 de 2015: integración de planes institucionales de seguridad al plan de acción.
Política Nacional de Confianza y Seguridad Digital (CONPES 3995 de 2020).

**Normatividad MinTIC:**
Decreto 1078 de 2015 - Sector TIC
Resolución MinTIC 2710 de 2017 – Política de Seguridad de la Información
Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC
Guía de Seguridad y Privacidad de la Información del MinTIC
Circular Externa 004 de 2016 - Política de Seguridad de la Información
Resolución 500 de 2021 del MinTIC: lineamientos y estándares para la estrategia de seguridad digital y adopción del MSPI.
Resolución 02277 de 2025 del MinTIC: actualización del Modelo de Seguridad y Privacidad

alineado con ISO/IEC 27001:2022.

**Estándares Técnicos:**
ISO/IEC 27001:2013 - Sistema de Gestión de Seguridad de la Información
ISO/IEC 27002:2013 - Código de buenas prácticas
NTC-ISO/IEC 27001 (Icontec)

## 2. POLÍTICA GENERAL Y ADOPCIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

### 2.1 DECLARACIÓN

La Política de Seguridad y Privacidad de la Información representa la posición de la administración de Distriseguridad con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros. la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Modelo de Seguridad y Privacidad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

### 2.2 PRINCIPIOS RECTORES

La Política de Seguridad y Privacidad de la Información se sustenta en los siguientes principios y/o características:

- Confidencialidad: la información debe estar accesible sólo a personas autorizadas.
- Integridad: la información debe ser completa, precisa y consistente.
- Disponibilidad: la información debe estar disponible cuando se requiera.
- Privacidad: protección de datos personales conforme a la ley.
- Audibilidad: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
- Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
- Cumplimiento legal: adecuación a normatividad aplicable.
- No repudio: Se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
- Legalidad: Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.
- Confiabilidad de la Información: Es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

La política será publicada, comunicada a todos los empleados y revisada anualmente.

## 2.3 OBJETIVOS

Para asegurar la dirección estratégica de Distriseguridad, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Proteger la confidencialidad, integridad y disponibilidad de la información
- Cumplir con requisitos legales y contractuales
- Garantizar la continuidad de servicios críticos para la seguridad ciudadana
- Proteger los datos personales según la Ley 1581 de 2012
- Prevenir, detectar y responder a incidentes de seguridad
- Minimizar el riesgo de los procesos misionales de la entidad.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Proteger los activos de información.
- 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 Distriseguridad.
- Garantizar la continuidad de la operación frente a incidentes.

## 2.4 NIVEL DE CUMPLIMIENTO

Este modelo aplica a todos los procesos, sistemas de información, infraestructura tecnológica, bases de datos, aplicaciones, y demás activos de información de Distriseguridad, así como a todos los funcionarios, contratistas, proveedores y terceros que tengan acceso a la información de la entidad.

A continuación, se establecen las políticas de seguridad que soportan el MSPI de Distriseguridad:

• Distriseguridad ha decidido definir, implementar, operar y mejorar de forma continua un Modelo de Seguridad y Privacidad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.

• Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.

• Distriseguridad protegerá la información generada, procesada o resguardada por los procesos y activos de información que hacen parte de los mismos.

• Distriseguridad protegerá la información creada, procesada, transmitida o resguardada por sus procesos, 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.

• Distriseguridad protegerá su información de las amenazas originadas por parte del personal.

• Distriseguridad protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

• Distriseguridad controlará la operación de sus procesos garantizando la seguridad de los recursos tecnológicos y las redes de datos.

• Distriseguridad implementará control de acceso a la información, sistemas y recursos de red.

• Distriseguridad garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

• Distriseguridad 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.

• Distriseguridad garantizará la disponibilidad de sus actividades y la continuidad de su operación basada en el impacto que pueden generar los eventos.

• Distriseguridad garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

• Distriseguridad garantizará el uso exclusivo de los correos electrónicos institucionales con el fin de resguardar la información suministrada en ellos, de Obligatorio cumplimientos para funcionarios y contratistas.

El incumplimiento a la política de Seguridad y Privacidad de la Información traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

## 3. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

### 3.1 Justificación

Distriseguridad Cartagena de Indias, 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, establece Distriseguridad que se compromete a proteger la información y los datos personales bajo su custodia, implementando controles de seguridad apropiados y garantizando el cumplimiento de la normatividad vigente en materia de protección de datos y seguridad de la información.

A los efectos de una correcta interpretación del presente Plan, se realizan las siguientes definiciones:

a) Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

b) Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

c) Tecnología de la Información: Se refiere al hardware y software operados la entidad o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

### 3.2 Objetivo

Definir los mecanismos y todas las medidas necesarias por parte de Distriseguridad, tanto técnica, lógica, física, legal y ambiental para la protección de los activos de información, los recursos y la tecnología de la entidad, con el propósito de evitar accesos no autorizados, divulgación, duplicación, interrupción de sistemas,

modificación, destrucción, pérdida, robo, o mal uso, que se pueda producir de forma intencional o accidental, frente a amenazas internas o externas, asegurando el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

### 3.3 Alcance

Este Plan de Seguridad y Privacidad de la Información y su política, son aplicables a todos los funcionarios de Distriseguridad, a sus recursos, contratistas, procesos y procedimientos tanto internos como externos, así mismo al personal vinculado a la entidad y terceras partes, que usen activos de información que sean propiedad de la entidad.

### 3.4 Cumplimiento

El cumplimiento de la Política de Seguridad y Privacidad de la Información es obligatorio. Si los funcionarios de la entidad o terceros violan este plan, Distriseguridad se reserva el derecho de tomar las medidas correspondientes.

### 3.5 Comunicación

Mediante socialización a todos los funcionarios de Distriseguridad se dará a conocer el contenido del documento de las políticas de seguridad, así mismo se deberá informar a los contratistas y/o terceros en el momento que se requiera con el propósito de realizar los ajustes y la retroalimentación necesaria para dar cumplimiento efectivo al plan.

Todos los funcionarios, contratistas y/o terceros de la entidad deben conocer la existencia de las políticas, la obligatoriedad de su cumplimiento, la ubicación física del documento estará a cargo del Sistema de Gestión Integrado para que sean consultados en el momento que se requieran, igualmente estarán alojados en la página de la entidad www.distriseguridad.gov.co.

### 3.6 Monitoreo

Se crearán los mecanismos y los indicadores correspondientes a la política de seguridad con el fin de determinar el cumplimiento de las mismas para establecer qué modificaciones o adiciones deben hacerse, este monitoreo debe realizarse como mínimo una vez al año o cuando sea necesario.

## 4. DESCRIPCIÓN DE LAS POLÍTICAS

**Generalidades**

Distriseguridad en todas sus áreas y procesos cuenta con información, reservada, relevante, privilegiada e importan ante, es decir que esta información es el principal activo de la entidad para el desarrollo de todas sus actividades por lo que se hace necesario y se debe proteger conforme a los criterios y principios de los sistemas de información, como son integridad, disponibilidad y confidencialidad de la información.

De acuerdo a esta Política se divulgan los objetivos y alcances de seguridad de la información de la entidad, que se logran por medio de la aplicación de controles de seguridad, con el fin de mantener y gestionar el riesgo como lo establece la política de riesgos institucional. Este documento tiene el objetivo de garantizar la continuidad de los servicios, minimizar la probabilidad de explotar las amenazas, y asegurar el eficiente Cumplimiento de los objetivos institucionales y de las obligaciones legales conforme al ordenamiento jurídico vigente y los requisitos de seguridad destinados a impedir infracciones y violaciones de seguridad.

### 4.1 Gestión de Activos

#### 4.1.1 Política para la identificación, clasificación y control de activos de información

Distriseguridad a través del Comité realizara la supervisión de cada proceso, el cual debe aprobar el inventario de los activos de información que procesa y produce la entidad, estas características del inventario deben establecer la clasificación, valoración, ubicación y acceso de la información, correspondiendo a Gestión de TIC y a Gestión Documental brindar herramientas que permitan la administración del inventario por cada área, garantizando la disponibilidad, integridad y confidencialidad de los datos que lo componen.

El líder del proceso de gestión tics, el facilitador del proceso de Gestión de Recursos Físicos con apoyo del ingeniero de sistemas tiene la responsabilidad de mantener el inventario completo y actualizado de los recursos de hardware y software de la entidad.

Pautas para tener en cuenta

a) Los usuarios deben acatar los lineamientos guía de clasificación de la Información para el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física de la entidad.

b) La información física y digital de Distriseguridad debe tener un periodo de almacenamiento que puede ser dictaminado por requerimientos legales o misionales; este período debe ser indicado en las tablas de retención documental y cuando se cumpla el periodo de conservación, se le debe dar el tratamiento de acuerdo a la disposición final definida por la entidad.

c) Los usuarios deben tener en cuenta estas consideraciones cuando impriman, escaneen, saquen copias y envíen faxes: verificar las áreas adyacentes a impresoras, escáneres, fotocopiadoras y máquinas de fax para asegurarse que no quedaron documentos relacionados o adicionales; asimismo, recoger de las impresoras, escáneres, fotocopiadoras y máquinas de fax, inmediatamente los documentos confidenciales para evitar su divulgación no autorizada o mal intencionada.

d) Tanto los funcionarios como el personal provisto por terceras partes deben asegurarse de que, en el momento de ausentarse de su puesto de trabajo, sus escritorios se encuentren libres de documentos y medios de almacenamiento, utilizados para el desempeño de sus labores; estos deben contar con las protecciones de seguridad necesarias de acuerdo con su nivel de clasificación.

e) La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y resguardo.

## 4.2 Control de Acceso

### 4.2.1 Política de acceso a redes y recursos de red

El ingeniero de sistemas TIC de Distriseguridad, como responsable de las redes de datos y los recursos de red de la entidad, debe propender porque dichas redes sean debidamente protegidas contra accesos no autorizados a través de mecanismos de control de acceso lógico.

**Pautas para tener en cuenta**

a) El proceso Gestión de TIC debe asegurar que las redes inalámbricas de Distriseguridad cuenten con métodos de autenticación que evite accesos no autorizados.

b) El proceso Gestión de TIC debe establecer controles para la identificación y autenticación de los usuarios provistos por terceras partes en las redes o recursos de red de Distriseguridad, así como velar por la aceptación de las responsabilidades de dichos terceros. Además, se debe formalizar la aceptación de las Políticas de Seguridad de la Información por parte de estos.

c) Los funcionarios y personal provisto por terceras partes, antes de contar con acceso lógico por primera vez a la red de datos de Distriseguridad, deben contar con el formato de creación de cuentas de usuario debidamente autorizado y el acuerdo de Confidencialidad firmado previamente.

d) Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos de Distriseguridad deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

### 4.2.2 Política de administración de acceso de usuarios

Distriseguridad establecerá privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información de la Entidad. Así mismo, velará porque los funcionarios y el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y porque la asignación de los derechos de acceso esté regulada por normas establecidas para tal fin.

**Pautas para tener en cuenta**

a) El proceso Gestión de TIC, debe definir lineamientos para la configuración de contraseñas que aplicarán sobre la plataforma tecnológica, los servicios de red y los sistemas de información de Distriseguridad; dichos lineamientos deben considerar aspectos como longitud, complejidad, cambio periódico, control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso, entre otros.

b) El proceso Gestión de TIC debe establecer un protocolo que asegure la eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre los recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna, cuando los funcionarios se desvinculan, toman licencias, vacaciones, son trasladados o cambian de cargo.

c) El proceso Gestión de TIC debe asegurarse que los usuarios o perfiles de usuario que tienen asignados por defecto los diferentes recursos de la plataforma tecnológica sean inhabilitados o eliminados.

d) Es responsabilidad de los propietarios de los activos de información, definir los perfiles de usuario y autorizar, conjuntamente con el proceso Gestión de TIC, las solicitudes de acceso a dichos recursos de acuerdo con los perfiles establecidos.

e) Los propietarios de los activos de información deben verificar y ratificar anualmente todas las autorizaciones sobre sus recursos tecnológicos y sistemas de información.

### 4.2.3 Políticas de control de acceso a sistemas de información y aplicativos.

Distriseguridad como propietario de los sistemas de información y aplicativos que apoyan los procesos y áreas que lideran, velarán por la asignación, modificación y revocación de privilegios de accesos a sus sistemas o aplicativos de manera controlada.

El proceso Gestión de TIC, como responsable de la administración de dichos sistemas de información y aplicativos, propende para que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico. Así mismo,

vela porque los desarrolladores, tanto internos como externos, acojan buenas prácticas de desarrollo en los productos generados para controlar el acceso lógico y evitar accesos no autorizados a los sistemas administrados.

**Pautas para tener en cuenta**

a) Los propietarios de los activos de información deben autorizar los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles establecidos y las necesidades de uso, acogiendo los procedimientos establecidos.

b) Los propietarios de los activos de información deben monitorear anualmente los perfiles definidos en los sistemas de información y los privilegios asignados a los usuarios que acceden a ellos.

c) El proceso Gestión de TIC debe establecer un protocolo para la asignación de accesos a los sistemas y aplicativos de Distriseguridad.

d) El proceso Gestión de TIC debe establecer el protocolo y los controles de acceso a los ambientes de producción de los sistemas de información; así mismo, debe asegurarse que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.

e) El proceso Gestión de TIC debe proporcionar repositorios de archivos fuente de los sistemas de información; estos deben contar con acceso controlado y restricción de privilegios, además de un registro de acceso a dichos archivos.

f) Los desarrolladores deben asegurar que los sistemas de información construidos requieran autenticación para todos los recursos y páginas, excepto aquellas específicamente clasificadas como públicas.

g) Los desarrolladores deben certificar que no se almacenen contraseñas, cadenas de conexión u otra información sensible en texto claro y que se implementen controles de integridad de dichas contraseñas.

h) Los desarrolladores deben establecer los controles de autenticación de tal manera que cuando fallen, lo hagan de una forma segura, evitando indicar específicamente cual fue la falla durante el logueo.

### 4.2.4 Políticas de seguridad física

Distriseguridad provee la implantación y vela por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones en todas sus áreas. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se considera áreas de acceso restringido.

Se debe tener acceso controlado y restringido a donde se encuentra los servidores y la zona de comunicaciones.

El proceso Gestión de TIC mantiene las normas, controles y registros de acceso a dichas áreas.

**Pautas para tener en cuenta**

a) Las solicitudes de acceso al área donde se encuentra el servidor o los centros de cableado deben ser aprobadas por funcionarios que apoyan el proceso Gestión de TIC autorizados; no obstante, los visitantes siempre deberán estar acompañados de un funcionario.

b) El proceso Gestión de TIC debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado.

c) El director debe proporcionar los recursos necesarios para ayudar a proteger, regular y velar por el perfecto estado de los controles físicos implantados en las instalaciones de Distriseguridad.

d) El director debe identificar mejoras a los mecanismos implantados y de ser necesario, la implementación de nuevos mecanismos, con el fin de proveer la seguridad física de las instalaciones de la entidad.

e) Los ingresos y egresos de personal a las instalaciones de Distriseguridad en horarios no laborales deben ser registrados; por consiguiente, los funcionarios y personal provisto por terceras partes deben cumplir completamente con los controles físicos implantados.

f) Los funcionarios deben portar el carné que los identifica como tales en un lugar visible mientras se encuentren en las instalaciones de Distriseguridad; en caso de pérdida del carné, deben reportarlo a la mayor brevedad posible.

g) Aquellos funcionarios o personal provisto por terceras partes para los que aplique, en razón del servicio prestado, deben utilizar prendas distintivas que faciliten su identificación.

### 4.2.5 Política de seguridad para los equipos

Distriseguridad, para evitar la pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica de la entidad que se encuentren dentro o fuera de sus instalaciones, proveerá los recursos que garanticen la mitigación de riesgos sobre dicha plataforma tecnológica.

**Pautas para tener en cuenta**

a) El proceso Gestión de TIC debe proveer los mecanismos y estrategias necesarios para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones de Distriseguridad.

b) El proceso Gestión de TIC debe realizar soportes técnicos y velar que se efectúen los mantenimientos preventivos y correctivos de los recursos de la plataforma tecnológica de la entidad.

c) El proceso Gestión de TIC en conjunto con el facilitador del proceso Gestión de Recursos Físicos debe propender porque las áreas de carga y descarga de equipos de cómputo se encuentren aisladas del área donde se ubica el servidor y otras áreas de procesamiento de información.

d) El proceso Gestión de TIC debe generar estándares de configuración segura para los equipos de cómputo de los funcionarios de la entidad y configurar dichos equipos acogiendo los estándares generados.

e) El proceso Gestión de TIC debe establecer las condiciones que deben cumplir los equipos de cómputo de personal provisto por terceros, que requieran conectarse a la red de datos de la entidad y verificar el cumplimiento de dichas condiciones antes de conceder a estos equipos acceso a los servicios de red.

f) El proceso Gestión de TIC debe generar y aplicar lineamientos para la disposición segura de los equipos de cómputo de los funcionarios de la entidad, ya sea cuando son dados de baja o cambian de usuario.

g) El proceso Gestión de Recursos Físicos debe velar porque la entrada y salida de estaciones de trabajo, servidores, equipos portátiles y demás recursos tecnológicos institucionales de las instalaciones de Distriseguridad cuente con la autorización documentada y aprobada previamente por el área.

h) El proceso Gestión de Recursos Físicos debe velar porque los equipos que se encuentran sujetos a traslados físicos fuera de la entidad y posean las pólizas de seguro.

i) El proceso Gestión de TIC es la única área autorizada para realizar movimientos y asignaciones de recursos tecnológicos; por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier funcionario de los recursos tecnológicos de Distriseguridad.

j) Las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos asignados a los funcionarios y personal provisto por terceras partes deben acoger las instrucciones técnicas que proporcione el proceso Gestión de TIC.

k) Cuando se presente una falla o problema de hardware o software u otro recurso tecnológico propiedad de la Institución, el usuario responsable debe informar al

facilitador del proceso Gestión de TIC, con el fin de realizar una asistencia adecuada. El usuario no debe intentar solucionar el problema.

l) La instalación, reparación o retiro de cualquier componente de hardware o software de las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos de la entidad, solo puede ser realizado por los profesionales universitarios de apoyo al proceso Gestión de TIC.

m) Los equipos de cómputo, bajo ninguna circunstancia, no deben ser dejados desatendidos en lugares públicos o a la vista, en el caso de que estén siendo transportados.

n) Los equipos de cómputo deben ser transportados con las medidas de seguridad apropiadas, que garanticen su integridad física.

o) Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.

p) En caso de pérdida o robo de un equipo de cómputo, se debe informar de forma inmediata al líder del proceso para que se inicie el trámite interno y se debe poner la denuncia ante la autoridad competente.

q) Los funcionarios de la entidad y el personal provisto por terceras partes deben asegurar que sus escritorios se encuentran libres de los documentos que son utilizados durante el desarrollo de sus funciones al terminar la jornada laboral y, que estos sean almacenados bajo las protecciones de seguridad necesarias.

### 4.2.6 Política de uso adecuado de internet

Distriseguridad consciente de la importancia del servicio de Internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en la entidad

**Pautas para tener en cuenta**

a) El proceso Gestión de TIC debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.

b) El proceso Gestión de TIC debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.

c) El proceso Gestión de TIC debe monitorear continuamente el canal o canales del servicio de Internet.

d) El proceso Gestión de TIC debe establecer e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.

e) El proceso Gestión de TIC debe generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar el monitoreo sobre la utilización del servicio de Internet.

f) Los usuarios del servicio de Internet de Distriseguridad deben hacer uso del mismo en relación con las actividades laborales que así lo requieran.

g) Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores.

h) No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este documento.

i) Los usuarios del servicio de internet tienen prohibido el acceso y el uso de servicios interactivos o mensajería instantánea como Kazaa, MSN, Yahoo, Net2phome y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias de Distriseguridad. Con excepciones del personal de comunicaciones.

j) No está permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el facilitador del proceso Gestión de TIC o a quien haya sido delegada de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

k) No está permitido el intercambio no autorizado de información de propiedad de Distriseguridad, de los funcionarios, con terceros.

### 4.2.7 Seguridad en Operaciones

Con el fin de garantizar la protección efectiva de los activos de información en las operaciones de la Entidad se tendrán en cuenta los siguientes principios:

**Gestión de Cambios:**

Los cambios se realizarán en un proceso formal para sistemas críticos pasando por pruebas en ambiente de desarrollo antes de producción y documentando los mismos, teniendo en cuenta siempre la activación de plan de respaldo para revertir cambios problemáticos

**Gestión de Vulnerabilidades:**

La seguridad parte del conocimiento de los niveles de exposición de la información de la entidad es por esto que se deben generar escaneos de vulnerabilidades anuales completos, así mismo los equipos deben estar configurados para la aplicación automáticas de parches de sistemas operativos.

**Protección contra Malware:**

Todos los equipos de la entidad deben contar con antivirus en todos los equipos con actualización automática adicionalmente con análisis completo semanal programado y bloqueo de dispositivos USB no autorizados.

**Seguridad en las Comunicaciones:**

Los accesos a los sistemas web d ela organización deben estar con cifrado de Información HTTPS para todas las aplicaciones coma también Cifrado de correos electrónicos con información sensible.

**Desarrollo con Terceros:**

Para los sistemas desarrollados por terceros se debe tener en cuenta:

- Cláusulas de seguridad en contratos
- Código fuente auditado antes de aceptación

## 5. PRIVACIDAD Y CONFIDENCIALIDAD

### 5.1 Política de tratamiento y protección de datos personales

En cumplimiento de la de Ley 1581 de 2012 y reglamentada parcialmente por el Decreto Nacional 1377 de 2013, por la cual se dictan disposiciones para la protección de datos personales, a través del Comité, Distriseguridad, propende por la protección de los datos personales de sus beneficiarios, proveedores y demás terceros de los cuales reciba y administre información.

Se establece los términos, condiciones y finalidades para las cuales Distriseguridad, como responsable de los datos personales obtenidos a través de sus distintos canales de atención, tratará la información de todas las personas que, en algún momento, por razones de la actividad que desarrolla la entidad, haya suministrado datos personales. En caso de delegar a un tercero el tratamiento de datos personales, Distriseguridad exigirá al tercero la implementación de los lineamientos y procedimientos necesarios para la protección de los datos personales. Así mismo, busca proteger la privacidad de la información personal de sus funcionarios, estableciendo los controles necesarios para preservar aquella información de la entidad conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias de la entidad y no sea publicada, revelada o entregada a funcionarios o terceras partes sin autorización.

**Pautas para tener en cuenta**

a) Las Unidades de Gestión que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben obtener la autorización para el tratamiento de estos datos con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de la entidad.

b) Las Unidades de Gestión que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben asegurar que solo aquellas personas que tengan una necesidad laboral legítima puedan tener acceso a dichos datos.

c) Las Unidades de Gestión que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben establecer condiciones

contractuales y de seguridad a las entidades vinculadas o aliadas delegadas para el tratamiento de dichos datos personales.

d) Las Unidades de Gestión que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos para el intercambio de estos datos con los terceros delegados para el tratamiento de dichos datos personales.

e) Las Unidades de Gestión que procesan datos personales de beneficiarios, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos para enviar a los beneficiarios, proveedores u otros terceros mensajes, a través de correo electrónico y/o mensajes de texto.

f) El comité debe establecer los controles para el tratamiento y protección de los datos personales de los beneficiarios, funcionarios, proveedores y demás terceros de Distriseguridad de los cuales reciba y administre información.

g) El proceso Gestión de TIC debe implantar los controles necesarios para proteger la información personal de los beneficiarios, funcionarios, proveedores u otras terceras partes almacenada en bases de datos o cualquier otro repositorio y evitar su divulgación, alteración o eliminación sin la autorización requerida.

h) Los usuarios y funcionarios deben guardar la discreción correspondiente, o la reserva absoluta con respecto a la información de la entidad o de sus funcionarios de cual tengan conocimiento en el ejercicio de sus funciones.

i) Es deber de los usuarios y funcionarios, verificar la identidad de todas aquellas personas, a quienes se les entrega información por teléfono, por fax, por correo electrónico o por correo certificado, entre otros.

j) Los usuarios de los portales de Distriseguridad deben asumir la responsabilidad individual sobre la clave de acceso a dichos portales que se les suministre; así mismo, deben cambiar de manera periódica esta clave de acceso.

Para el Cumplimiento de la Ley 1581 de 2012 se tendrán en cuenta los siguientes Principios de Tratamiento:

- Legalidad
- Finalidad
- Libertad
- Veracidad o calidad
- Transparencia
- Acceso y circulación restringida
- Seguridad

- Confidencialidad

Con respecto a las Bases de Datos con Información Personal se deberá revisar anualmente el Inventario de Bases de Datos y específicamente:

- Base de datos de funcionarios y contratistas
- Registros de visitantes a áreas de protección especial
- Bases de datos de contactos ciudadanos
- Información de sistemas de videovigilancia con reconocimiento facial (si aplica)
- Registros de acceso a instalaciones

Los titulares de datos personales tienen derecho a:

- Conocer, actualizar y rectificar sus datos
- Solicitar prueba de la autorización otorgada
- Ser informado sobre el uso de sus datos
- Presentar quejas ante la Superintendencia
- Revocar la autorización y solicitar supresión de datos
- Acceder gratuitamente a sus datos

Con respecto a la Obtención de Autorización, este debe ser:

- Previa, expresa e informada
- Por escrito, verbal o conducta inequívoca
- Clara sobre finalidad del tratamiento
- Archivo de autorizaciones por tiempo de tratamiento + 10 años

Los Avisos de Privacidad tendrán las siguientes características:

- Publicado en sitio web institucional
- Visible en formularios de captura de datos
- Contenido: identidad del responsable, tratamiento, derechos y canal de atención

### 5.2 Disponibilidad del servicio e información

Distriseguridad, con el propósito de garantizar la disponibilidad de la información y mantener los servicios orientados con el objetivo de la entidad y los ofrecidos externamente, ha decidido crear una política para proveer el funcionamiento correcto y seguro de la información y medios de comunicación.

**Política de continuidad, contingencia y recuperación de la información**

Distriseguridad proporcionará los recursos suficientes para facilitar una respuesta efectiva a los funcionarios y para los procesos en caso de contingencia o eventos catastróficos que se presenten en la entidad y que afecten la continuidad de su operación y servicio.

**Copias de Seguridad**

Toda información que pertenezca a la matriz de activos de información institucional o que sea de interés para un proceso operativo o de misión crítica debe ser respaldada por copias de seguridad tomadas de acuerdo a los procedimientos documentados por el Comité. Dicho procedimiento debe incluir las actividades de almacenamiento de las copias en sitios seguros.

Las dependencias de Distriseguridad deben realizar pruebas controladas para asegurar que las copias de seguridad pueden ser correctamente leídas y restauradas.

Los registros de copias de seguridad deben ser guardados en una base de datos creada para tal fin.

El proceso Gestión de TIC debe proveer las herramientas para que las dependencias puedan administra la información y registros de copias de seguridad. La (el) profesional especializado con funciones de Control Interno debe efectuar auditorías aleatorias que permitan determinar el correcto funcionamiento de los procesos de copia de seguridad.

La creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios.

**Funciones del comité**

a) El Comité, debe reconocer las situaciones que serán identificadas como emergencia o desastre para la entidad, los procesos o las áreas y determinar cómo se debe actuar sobre las mismas.

b) El Comité, debe liderar los temas relacionados con la continuidad de la entidad y la recuperación ante desastres.

c) El Comité debe realizar los análisis de impacto a la entidad y los análisis de riesgos de continuidad para, posteriormente proponer posibles estrategias de recuperación en caso de activarse el plan de contingencia o continuidad, con las consideraciones de seguridad de la información a que haya lugar.

d) El Comité debe validar que los procedimientos de contingencia, recuperación y retorno a la normalidad incluyan consideraciones de seguridad de la información.

e) El Comité, debe asegurar la realización de pruebas periódicas del plan de recuperación ante desastres y/o continuidad de entidad, verificando la seguridad de la información durante su realización y la documentación de dichas pruebas.

PLAN DE ACCION DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DESDE EL ENFOQUE DE SEGURIDAD INFORMATICA SOBRE LOS ACTIVOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES FRENTE A CIBERAMENAZAS

| Líneas Estratégicas | Enfoque | Fecha Inicio | Fecha Final |
|---|---|---|---|
| Fortalecimiento del Modelo de gestión de seguridad y privacidad de la información | Activos de Información | 1-feb-26 | 31-dic-26 |
| | Riesgos de Seguridad de la Información | | |
| | Incidentes de Seguridad y Privacidad de la Información | | |
| | Seguimiento a vulnerabilidades | | |
| Fortalecimiento del plan de Continuidad de la operación de los servicios de la entidad | Continuidad del Negocio | 1/02/2026 | 31/12/2026 |
| Implementación del Programa Integral de Gestión de Datos Personales | Datos Personales | 1/02/2026 | 31/12/2026 |
| Fortalecimiento de las estrategias de Cambio, Cultura y Apropiación del Sistema de Gestión de Seguridad de la Información. | Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación | 1/02/2026 | 31/12/2026 |
| Planeación y seguimiento | Seguimiento y reporte del estado de las Acciones Correctivas, correcciones y Oportunidades de Mejora | 1/02/2026 | 31/12/2026 |