Sistema Integrado de Gestión

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Código: MGTICS - 001

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

1. ADOPCIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1.1 DECLARACIÓN

El presente Modelo de Seguridad y Privacidad de la Información establece el marco de referencia para la protección de los activos de información de Distriseguridad, garantizando la confidencialidad, integridad, disponibilidad y privacidad de los datos, en cumplimiento con la normatividad colombiana vigente, especialmente el Modelo de Seguridad y Privacidad de la Información (MSPI) establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC.

Este modelo está diseñado para proteger la información que la entidad gestiona en el marco de sus funciones misionales, garantizando el derecho fundamental del habeas data y la protección de datos personales de los ciudadanos, contratistas y funcionarios, en cumplimiento con la Ley 1581 de 2012 y sus decretos reglamentarios.

1.2 OBJETO

Establecer los lineamientos, directrices y controles de seguridad y privacidad de la información que deben implementarse en Distriseguridad para:

1Proteger los activos de información contra amenazas internas y externas

- Garantizar la continuidad de los servicios de la entidad
- Cumplir con los requisitos legales y regulatorios aplicables
- Gestionar adecuadamente los datos personales bajo custodia de la entidad
- Establecer una cultura de seguridad de la información

1.3 ALCANCE

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.

1.4 DEFINICIONES

Activo de Información: Cualquier información o elemento relacionado con el tratamiento de la misma que tenga valor para la organización.
Amenaza: Causa potencial de un incidente no deseado que puede resultar en daño a un sistema o a la organización.

Autenticación: Proceso de verificar la identidad de un usuario, proceso o dispositivo.
Confidencialidad: Propiedad de la información de no estar disponible o ser revelada a individuos, entidades o procesos no autorizados.
Dato Personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
Incidente de Seguridad: Evento o serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones del negocio.
Integridad: Propiedad de exactitud y completitud de la información.
MSPI: Modelo de Seguridad y Privacidad de la Información establecido por MinTIC.
Privacidad: Derecho de los individuos a controlar o influir sobre qué información relacionada con ellos puede ser recolectada y almacenada.
Riesgo: Combinación de la probabilidad de un evento y sus consecuencias.
Titular: Persona natural cuyos datos personales sean objeto de tratamiento.
Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

1.5 PRINCIPIOS

El modelo 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.

2.0 POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2.1 DECLARACIÓN DE LA POLÍTICA

Distriseguridad 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.

2.2 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.

2.3 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.

2.4 ROLES Y RESPONSABILIDADES

ROL	RESPONSABILIDADES CLAVE
Dirección General	Liderar el compromiso organizacional con la seguridad. Aprobar el PSPI y asignar recursos.
Responsable de Seguridad de la Información (CISO o equivalente)	Coordinar implementación, revisión actualización del plan. Gestionar incidentes de seguridad
Oficial de Privacidad de Datos	Gestionar cumplimiento de políticas de tratamiento y protección de datos personales. Garantizar cumplimiento de Ley 1581 de 2012 Atender peticiones, quejas y reclamos sobre datos personales Coordinar con áreas responsables del tratamiento de datos
Responsables de procesos y tecnología	Aplicar controles definidos y asegurar cumplimiento operacional.
Usuarios y terceros	Cumplir con políticas y reportar incidentes.

4 CONTROLES DE SEGURIDAD

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 con este Modelo 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.

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.

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.

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.

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.

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.

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

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 de la 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

4.2.8 Disponibilidad del servicio de 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.

5. GESTIÓN DE INCIDENTES

Definición de Incidente

Se considera incidente de seguridad cualquier evento que comprometa o tenga el potencial de comprometer la confidencialidad, integridad o disponibilidad de la información, incluyendo pero no limitado a:

- Acceso no autorizado a sistemas o información
- Fuga o pérdida de datos personales o confidenciales
- Infección por malware o ransomware
- Ataques de phishing o ingeniería social exitosos
- Denegación de servicio
- Modificación no autorizada de información
- Pérdida o robo de equipos
- Violaciones a políticas de seguridad

Proceso de Gestión de Incidentes

Todo incidente de seguridad será gestionado siguiendo las siguientes fases:

Detección y Reporte: Identificar y reportar inmediatamente el incidente al Oficial de Seguridad
Clasificación y Priorización: Evaluar la severidad y el impacto del incidente
Contención: Aislar los sistemas afectados para evitar propagación
Investigación: Determinar la causa raíz y el alcance del incidente
Erradicación: Eliminar la amenaza y las vulnerabilidades explotadas
Recuperación: Restaurar los sistemas y servicios afectados
Lecciones Aprendidas: Documentar el incidente y mejorar los controles

Notificación de Brechas de Datos Personales

En caso de violación de datos personales, la entidad cumplirá con los siguientes plazos establecidos por la normatividad:

- Notificar a la Superintendencia de Industria y Comercio dentro de los 15 días hábiles siguientes
- Informar a los titulares afectados de manera inmediata
- Documentar detalladamente el incidente, su alcance y las medidas adoptadas
- Implementar medidas correctivas para prevenir futuras ocurrencias

6. PLAN DE CONTINUIDAD

La entidad debe contar con un Plan de Continuidad del Negocio (PCN) que asegure la disponibilidad de los servicios críticos ante eventos disruptivos. El plan incluirá:

- Análisis de impacto al negocio (BIA) para identificar procesos críticos
- Objetivos de tiempo de recuperación (RTO) y punto de recuperación (RPO)
- Estrategias de recuperación de sistemas y datos
- Procedimientos de respaldo y restauración
- Sitio alterno o plan de trabajo remoto
- Esquemas de comunicación en situaciones de crisis
- Roles y responsabilidades durante la contingencia

7. PRIVACIDAD Y CONFIDENCIALIDAD

7.1 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.

7.2 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.

8. CUMPLIMIENTO Y AUDITORÍA

8.1 Auditorías de Seguridad

Se realizarán auditorías periódicas para verificar el cumplimiento de este modelo y la efectividad de los controles implementados:

- Auditorías internas: al menos una vez al año
- Auditorías externas: cuando lo requiera la normatividad o la alta dirección
- Revisiones de cumplimiento normativo: continuas
- Pruebas de penetración: Anuales
- Evaluaciones de vulnerabilidades: Semestrales

8.2 Indicadores de Gestión

Se establecerán indicadores para medir la efectividad del modelo, incluyendo:

- Número de incidentes de seguridad reportados y resueltos
- Tiempo promedio de respuesta a incidentes
- Porcentaje de cumplimiento en aplicación de parches
- Nivel de concienciación del personal (resultados de capacitaciones)
- Porcentaje de activos inventariados y clasificados
- Cumplimiento de objetivos RTO y RPO
- Número de vulnerabilidades críticas pendientes

8.3 No Conformidades

Cualquier incumplimiento a las políticas de seguridad será documentado, investigado y sujeto a las acciones correctivas correspondientes, que pueden incluir:

- Capacitación y sensibilización adicional
- Amonestaciones verbales o escritas
- Suspensión de privilegios de acceso
- Medidas disciplinarias según el reglamento interno
- Acciones legales en casos graves

8.4 REVISIÓN Y ACTUALIZACIÓN DEL MODELO

Este Modelo de Seguridad y Privacidad de la Información será revisado y actualizado:

- Al menos una vez al año o cuando cambien las condiciones del entorno
- Cuando se identifiquen cambios normativos significativos
- Después de incidentes mayores de seguridad
- Cuando se implementen nuevas tecnologías o servicios
- Como resultado de auditorías o evaluaciones de riesgos

Las actualizaciones al modelo serán aprobadas por la alta dirección y comunicadas oportunamente a todos los funcionarios y partes interesadas.