PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Contenido

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. Introducción

El Plan de seguridad de la información constituye una parte fundamental del Modelo de Seguridad y Privacidad de la Información (MSPI) de Gobierno Digital y se convierte en la base para la implementación de los controles, procedimientos y estándares definidos.

El Desarrollo de este plan está basado en el Modelo de Seguridad de y Privacidad de la Información expuesto por el Ministerio de la Tecnologías de la Información y las Comunicaciones, el cual recopila las mejores prácticas para suministrar requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo; lo anterior teniendo en cuenta las necesidades y objetivos, los requisitos de seguridad, los procesos misionales y el tamaño y estructura de la Administración Municipal de Caldas, Antioquia.
De esta forma estamos dando cumplimiento al decreto único reglamentario 1078 de 2015 en el componente de seguridad y privacidad de la Información como parte integral de la estrategia de Gobierno Digital.

Las políticas incluidas en este plan se convierten en la base para implementar controles en la Información misional de la Administración Municipal de Caldas, Antioquia.

2. Marco Legal

NORMA	DESCRIPCIÓN
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
NTC / ISO 27001:2013	Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).
NTC/ISO 27002:2013	Tecnología de la información. Técnicas de seguridad. Código de Práctica para controles de seguridad de la información.

Alineación con el Plan de Desarrollo Municipal

LÍNEA ESTRATÉGICA	**COMPONENTE**	**PROGRAMA**	**PRODUCTO**
Gobernanza para la transformación de la esperanza en confianza ciudadana	Transparencia, rendición de cuentas y legalidad	Gobierno digital y sistemas de información ciudadana	Acciones para Cofinanciar la modernización tecnológica de la administración municipal y las entidades descentralizadas

3. Alcance

Todas las políticas de seguridad de la información, aquí contenidas, serán aplicadas a los procesos estratégicos, misionales, de apoyo y de evaluación de la Administración Municipal y deberán ser conocidas y cumplidas por todos los funcionarios, contratistas, proveedores, ciudadanía en general y demás partes interesadas, que accedan a los sistemas de información e instalaciones físicas.

4. Direccionamiento Estratégico

- **Misión**

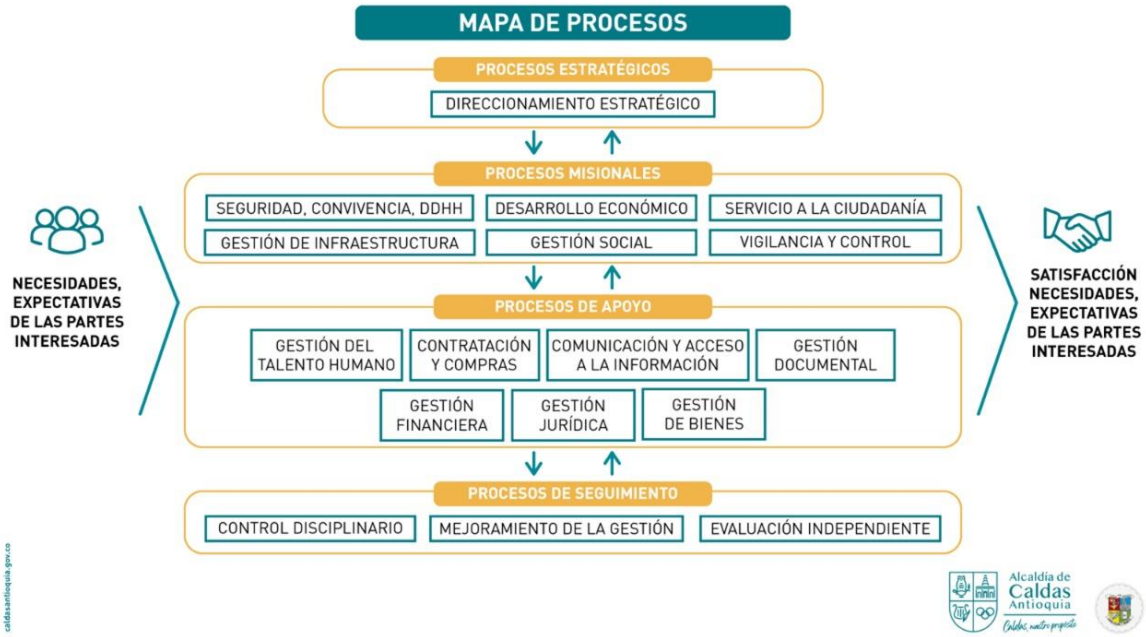
  La Alcaldía de Caldas, como entidad territorial, promueve y aporta al desarrollo integral para hacer de Caldas un municipio transformador, que enfrenta las diferentes formas de exclusión social, por medio del talento humano competente y con vocación de servicio, haciendo un uso adecuado y efectivo de los recursos públicos, contribuyendo a la sostenibilidad del municipio y mejorando la calidad de vida de los habitantes y de los diferentes grupos de valor.

- **Visión**
  Caldas, en el año 2024, será un territorio transformado a nivel social, económico, tecnológico y ambiental, con la capacidad técnica, administrativa y operacional. Será un municipio incluyente, transparente, saludable, con un ordenamiento sostenible, al servicio del bienestar y mejoramiento de la calidad de vida de la población.

- **Política Sistema Integrado de Gestión**

  La Alcaldía de Caldas está comprometida con el mejoramiento de la calidad de vida de los habitantes del municipio, mediante la formulación y ejecución de planes, programas y proyectos que estén orientados en realizar acciones tendientes a resolver las necesidades de las partes interesadas de manera ágil y eficiente en el marco de la legalidad, transparencia e integralidad, mediante una gestión participativa, el adecuado uso de los recursos y finanzas públicas, el compromiso por el bienestar físico, mental y social de los servidores, fortaleciendo la institucionalidad y el mejoramiento continuo de los procesos, los cuales están soportados en el cumplimiento permanente de los requisitos legales.

- **Mapa de Procesos**



5. Términos y Definiciones

- **Acceso a la Información Pública:** derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).
- **Activo:** en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).
- **Activo de Información:** cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de la Administración Municipal y, en consecuencia, debe ser protegido. Se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- **Amenaza:** es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la Seguridad Informática, los elementos de información. Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

- **Análisis de riesgos de seguridad de la información:** proceso sistemático de identificación de fuentes, estimación de impactos, probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.
- **Archivo:** conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).
- **Auditoría:** proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).
- **Autenticación:** es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.
- **Autorización:** consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).
- **Bases de Datos Personales:** conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)
- **Ciberseguridad:** capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).
- **Ciberespacio:** es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
- **Confidencialidad:** es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.
- **Control:** son 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 es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Datos Abiertos:** son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier

ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)

- **Datos Personales:** cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012)
- **Datos Personales Públicos:** es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)
- **Datos Personales Privados:** es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)
- **Datos Personales Mixtos:** para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.
- **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. (Decreto 1377 de 2013, art 3)
- **Declaración de aplicabilidad:** documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).
- **Derecho a la Intimidad:** derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).
- **Disponibilidad:** es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.
- **Encargado del Tratamiento de Datos:** persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3).

- **Gestión de incidentes de seguridad de la información:** es el conjunto de procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
- **Información Pública Clasificada:** es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).
- **Información Pública Reservada:** es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).
- **Integridad:** es la protección de la exactitud y estado completo de los activos de información.
- **Ley de Habeas Data:** se refiere a la Ley Estatutaria 1266 de 2008.
- **Ley de Transparencia y Acceso a la Información Pública:** Se refiere a la Ley Estatutaria 1712 de 2014.
- **Mecanismos de protección de datos personales:** lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.
- **Partes interesadas (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 continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
- **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. (ISO/IEC 27000).
- **Privacidad:** en el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.
- **Propietarios de los activos de información:** son los responsables de cada uno de los activos de información (archivos, bases de datos, contratos y acuerdos,

documentación del sistema, manuales de usuario, material de formación, aplicaciones, software del sistema, equipos informáticos, equipos de comunicaciones, servicios informáticos y de comunicaciones, las personas, etc. Esta persona se hará cargo de mantener la seguridad del activo.

- **Recursos tecnológicos:** son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo.
- **Registro Nacional de Bases de Datos:** directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25).
- **Responsabilidad Demostrada:** conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.
- **Responsable del Tratamiento de Datos:** 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. (Ley 1581 de 2012, art 3).
- **Riesgo:** posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Seguridad de la información:** preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- **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, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).
- **Sistema de información (SI)**: es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo. Dichos elementos pueden ser personas, actividades o técnicas de trabajo, datos y recursos materiales en general.
- **Titulares de la información:** personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)

- **Tratamiento de Datos Personales:** cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).
- **Trazabilidad:** cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).
- **Vulnerabilidad:** debilidad de un activo o de un control, que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

6. Objetivo General

Establecer las políticas de seguridad de la información para la Administración Municipal de Caldas Antioquia, con el fin de cumplir con los requisitos de seguridad, definidos en el MSPI que ayudarán, mediante su implementación, a preservar la Confidencialidad, Integridad y Disponibilidad de la información. De acuerdo a los lineamientos de buenas prácticas en Seguridad y Privacidad para las entidades del Estado, con el fin de regular la gestión de la seguridad de la información al interior de la entidad.

7. Partes Interesadas

Todos los funcionarios, contratistas, proveedores, entes de control, entidades gubernamentales del orden nacional, departamental y local, y ciudadanía en general que accedan a los sistemas de información e instalaciones físicas de la Administración Municipal.

8. Esquema del Plan

El Plan de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la Administración Municipal de Caldas Antioquia con respecto a la protección de los activos de información que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad 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.

9. Desarrollo del Plan

La Administración Municipal de Caldas Antioquia, para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y las acciones a implementar son:

- Minimizar el riesgo de los procesos misionales de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- 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 ciudadanía en general.
- Garantizar la continuidad del negocio frente a incidentes.

La Política de Seguridad que soportan el SGSI, considera los siguientes aspectos:

- La Administración Municipal de Caldas, Antioquia ha decidido **definir, implementar, operar y mejorar** de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.
- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.
- La Administración Municipal de Caldas, Antioquia:
    - Protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros.
    - Protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
    - Protegerá su información de las amenazas originadas por parte del personal.
    - Protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
    - Controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
    - Implementará control de acceso a la información, sistemas y recursos de red.
    - Garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

- 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.
- Garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- Garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

9.1 Plan de acción

Entregable	Responsable de actividad	Actividad	Periodicidad
Usuario - Clave	Informática	Creación, activación e inactivación de usuarios	A demanda
Contratos	Informática	Renovación de licenciamiento	Anual
Backup	Informática	Realizar backups diarios - BD	Diario
Evidencia del seguimiento	Informática	Configuración y seguimiento a la seguridad perimetral y consola antivirus.	Constante
Plan de Mantenimiento preventivo e Informe de la mesa de ayuda	Informática	Mantenimiento preventivo y/o correctivo a equipos de cómputo y demás elementos tecnológicos	Constante

10. Seguimiento del Plan

- Cada una de las dependencias deberá informar al área de informática acerca de las novedades de ingreso, retiro temporal o definitivo del personal que labora en la entidad, con el fin de asignar o eliminar los usuarios de red y sus respectivos permisos de acceso a la información. De igual manera, impedir el acceso no autorizado a la información mantenida por los sistemas y aplicaciones.
- En cuanto al Software, se garantiza la continuidad de los aplicativos que requieren renovación anual, con el fin de tener el licenciamiento legal y vigente.
- Programar y realizar mantenimientos periódicos preventivos a los equipos de cómputo y demás elementos tecnológicos de la entidad, así como los mantenimientos correctivos a los que haya lugar.
- Restringir los permisos de instalación, cambio o eliminación de componentes de la plataforma tecnológica de la Administración Municipal. Está prohibida 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. Este seguimiento se hace a través de reportes generados por la plataforma de seguridad perimetral.

- Realizar back ups diarios de las bases de datos de Saimyr y QX.
- Generar copias de seguridad de la información de los funcionarios que se retiran o cambian de labores, cuando es solicitado a través de la mesa de ayuda.
- Monitorear constantemente los aplicativos de seguridad de la información, Fortinet y Antivirus, con el fin de detectar y corregir cualquier anomalía en la plataforma tecnológica de la Administración Municipal.
- Garantizar la disponibilidad de la red de datos, realizando control de tráfico y estableciendo políticas que garanticen la integridad y confidencialidad de la información. Está prohibido el intercambio no autorizado de información de propiedad de la Administración Municipal entre sus funcionarios y contratistas con terceros.