RESOLUCIÓN No. 038
Del 30 de enero de 2020

"POR MEDIO DE LA CUAL SE ADOPTA EL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA ADMINISTRACIÓN CENTRAL MUNICIPAL DE PLATO MAGDALENA VIGENCIA 2020"

El Alcalde Del Municipio De Plato Magdalena, en uso de sus facultades legales conferidas por la constitución y la ley y en especial el decreto ley 1078 de 2015, y

CONSIDERANDO:

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

Que la Ley 1273 de 2009 modificó el Código Penal, creando un nuevo bien jurídico tutelado denominado "*De la Protección de la información y de los datos*" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones "TIC", entre otras disposiciones.

Que el Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de tecnologías de la Información y las Comunicaciones, contempló en el Artículo 2.2.9.1.2.2, los instrumentos para implementar la Estrategia de Gobierno en Línea, dentro de los cuales se exige la elaboración por parte de cada entidad de un Plan de Seguridad y Privacidad de la Información.

Que mediante Decreto 415 del 7 de marzo de 2016, se adicionó al Decreto 1083 de 2015, todo lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de Tecnologías de la Información y las Comunicaciones.

Que mediante el Decreto 612 de 4 de abril de 2018 se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.

Que mediante el Decreto 1008 de 14 de junio de 2018 se establece que la Seguridad y privacidad de la información es uno de los habilitadores transversales de la nueva Política de Gobierno Digital.

Que mediante el Plan de Seguridad y Privacidad de la Información se busca proteger la integridad y garantizar la disponibilidad y confidencialidad de todos los activos de información de la Administración Central Municipal de Plato.

Por lo expuesto el Alcalde de Plato,

RESUELVE:

ARTICULO PRIMERO. Adoptar el Plan de Seguridad y privacidad de la Información, Vigencia 2020 para la Administración Central Municipal de Plato (Magdalena), el cual forma parte integral del presente Acto Administrativo.

ARTICULO SEGUNDO. El Plan de Seguridad y Privacidad de la Información tiene como objetivo principal proteger la integridad y garantizar la disponibilidad y confidencialidad de la información de la Entidad.

ARTICULO TERCERO. La presente Resolución rige a partir de la fecha de su expedición.

PUBLÍQUESE Y CÚMPLASE

Dado en el Despacho del Alcalde del Municipio de Plato Magdalena, a los treinta (30) días del mes de enero de dos mil veinte (2020).

JAIME ALONSO PEÑA PEÑARANDA
Alcalde Municipal.

ELABORO:	VERIFICO:	APROBO:

PLAN DE SEGURIDAD Y PRIVACIDAD EN LA INFORMACIÓN

ADMINISTRACIÓN CENTRAL MUNICIPAL DE PLATO (MAGDALENA)

SECRETARIA DE **GOBIERNO**
ÁREA DE **SISTEMAS**

ENERO DE 2020

INTRODUCCIÓN

Las políticas de Seguridad y Privacidad de la Información definen los lineamientos en esta materia que se deben tener en cuenta en la Administración Municipal de Plato en el tratamiento de la información institucional, manteniendo sus principios de confidencialidad, integridad y disponibilidad, con orientación hacia la satisfacción de las necesidades de información de los distintos grupos de interés de la entidad, enmarcado dentro de la estrategia Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC.

En la actual y cambiante sociedad de la información, toda entidad pública o privada debe lograr una adecuada articulación entre el Sistema de Gestión de Seguridad de la Información –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 Administración Central Municipal de Plato. 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.

Este documento se constituye en un plan de privacidad y seguridad de la Información, debe estar alineado con el propósito misional de la entidad, con el fin de definir las acciones a implementar a nivel de seguridad y privacidad de la información, con la intención de garantizar el buen tratamiento de datos y de información y controlar el uso eficiente y correcto de dichos activos.

1. OBJETIVOS

1.1. Objetivo General

Identificar y ejecutar actividades orientadas a fortalecer el aseguramiento de los servicios de TI, así como la información que genera u obtiene la Administración Municipal de Plato, para preservar la confidencialidad, integridad y disponibilidad de la información relacionada con sus distintos usuarios o grupos de interés.

1.2. Objetivos Específicos

- ✓ Mantener la confianza de los ciudadanos en general y el compromiso de todos los funcionarios, contratistas o practicantes de la Administración Central Municipal de Plato, respecto al correcto manejo y protección de la información que es gestionada y resguardada en la Entidad.
- ✓ Identificar e implementar las tecnologías necesarias para fortalecer la función de la seguridad de la información.
- ✓ Proteger la información y los activos tecnológicos de la Institución.
- ✓ Asegurar la identificación y gestión de los riegos a los cuales se expone los activos de información de la Administración Municipal de Plato.
- ✓ Proteger la información y los activos tecnológicos de la Institución.
- ✓ Concientizar a los funcionarios, contratistas y practicantes de la Administración Municipal de Plato sobre el uso adecuado de los activos de información puestos a su disposición para la realización de las funciones y actividades diarias, garantizando la confidencialidad, la privacidad y la integridad de la información.

2. ALCANCE

Está determinado por las directrices y lineamientos en temas de seguridad y privacidad de la información y activos de información emitidos por el gobierno nacional y entidades competentes y por cumplimiento por parte de todos los

funcionarios, contratistas de la Administración Central Municipal de Plato (Magdalena) y demás personas que tengan acceso a información o tengan algún tipo de relación con la entidad.

3. POLÍTICAS DEL PLAN

Está determinado por las directrices y lineamientos en temas de seguridad y privacidad de la información y activos de información emitidos por el gobierno nacional y entidades competentes y por cumplimiento por parte de todos los funcionarios, contratistas de la Administración Central Municipal de Plato (Magdalena) y demás personas que tengan acceso a información o tengan algún tipo de relación con la entidad.

A continuación, se establecen las políticas que soportan el Plan de Seguridad y Privacidad de la Información de Administración Central Municipal de Plato:

- ☑ ***Implementación:*** La Administración Central Municipal de Plato 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.
- ☑ ***Responsabilidades***: 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.
- ☑ ***Protección de la Información por accesos otorgados al personal***: La Administración Central protegerá su información de las amenazas originadas por parte del personal.
- ☑ ***Protección de la Información por accesos otorgados a terceros***: La Administración Central 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, como proveedores o clientes, o como resultado de un servicio interno en outsourcing.

- ☑ ***Controles para la protección de la Información***: La Administración Central 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.
- ☑ ***Control de la operación:*** La Administración Central controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- ☑ ***Protección a la Infraestructura Tecnológica***: La Administración Central protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- ☑ ***Control de Acceso a la Información***: La Administración Central implementará control de acceso a la información, sistemas y recursos de red.
- ☑ ***Incorporación de la Seguridad en los sistemas de información***: La Administración Central garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- ☑ ***Mejora continua al modelo de seguridad***: La Administración Central 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.
- ☑ ***Disponibilidad y continuidad de la operación***: La Administración Central garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- ☑ ***Cumplimiento de Obligaciones***: La Administración Central garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

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.

4. REFERENCIA NORMATIVA

- ✓ Ley 527 de 1999: Se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación.
- ✓ Ley 1221 de 2008. 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 1266 de 2008: Se dictan las disposiciones generales del Habeas 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.
- ✓ Ley 1273 de 2009. Modifica el Código Penal, 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.
- ✓ Ley 1341 de 2009: Definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la información y las comunicaciones-TIC-, se crea la Agencia Nacional del Espectro.
- ✓ Ley 1712 de 2014: Crea la Ley de Transparencia y del derecho de acceso a la información pública nacional.
- ✓ Decreto 103 de 2015. 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.
- ✓ Decreto 1078 de 2015: Se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y la Comunicación.

- ✓ Decreto 1008 de 14 de junio de 2018. Se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

5. CONCEPTOS ASOCIADOS

- ✓ ***Activo***: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).
- ✓ ***Amenazas***: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- ✓ ***Análisis de riesgo***: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- ✓ ***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).
- ✓ ***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***: Ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701, Tomado de la Academia de la lengua española).
- ✓ ***Control***: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- ✓ ***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).
- ✓ ***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. (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)
- ✓ ***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).
- ✓ ***Trazabilidad***: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).
- ✓ ***Vulnerabilidad***: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).
- ✓ ***Persona interesada (Stakeholder):*** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

6. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

6.1. Acceso a la información

Tendrán acceso a la información disponible en la entidad, los empleados y funcionarios teniendo en cuenta las funciones y responsabilidades asignadas y los

contratistas según las actividades descritas en su contrato siempre y cuando la información sea necesaria para el desarrollo de las funciones y actividades según corresponda.

6.2. Usuarios y contraseñas

Para los sistemas de información o plataformas que necesiten de un usuario y contraseña para su acceso, serán administrados por el jefe de la dependencia que corresponda y este asignará bajo su responsabilidad usuarios a sus subordinados para la gestión de información en dichos sistemas o plataformas y tomará los respectivos correctivos en caso de ser necesario.

El jefe inmediato y el Área de Control Interno o quien haga sus veces como segunda y tercera línea de defensa realizará el seguimiento correspondiente con el fin de verificar que el control de usuarios y contraseñas sea efectivo.

6.3. Seguridad de la información

Los usuarios de la información (contratistas, funcionarios, terceros) son responsables de esta, cada vez que la entidad les suministre en cumplimiento de sus funciones y responderá por el correcto uso de esta de manera íntegra y confidencial.

La información que no haya sido autorizada para publicación por parte del representante de la entidad o los jefes de dependencia tendrán la calidad de reservada y su reproducción, edición, impresión y divulgación será prohibida. Cuando por algún motivo los usuarios mencionados rompan el *principio de confidencialidad* se tomarán los correctivos necesarios por parte de su superior inmediato.

Para garantizar la custodia de la información gestionada a través de correos electrónicos, serán utilizados solamente correos electrónicos institucionales para evitar que cuando haya cambio de personal se pierda información gestionada por medio de correos electrónicos personales.

6.4. Seguridad en las estaciones de trabajo

Cada funcionario y contratista al cual se le asigne un equipo de cómputo, deberá asignar una contraseña de acceso que contenga criterios de seguridad establecidos por la secretaría de Gobierno para evitar accesos no concedidos y perdida y/o edición de información sin autorización.

6.5. Seguridad software

Los softwares que sean adquiridos por la Administración Central Municipal, deberán contar con la licencia legal correspondiente y su uso deberá tener restricciones tales como usuarios y contraseñas para evitar el acceso, edición, eliminación y divulgación de la información que se gestiona.

6.6. Equipos de cómputo

Los funcionarios solo utilizarán equipos de cómputo de propiedad de la Administración Central Municipal. En caso de que se vaya a utilizar un equipo personal deberá solicitar permiso para su utilización con su jefe inmediato o el secretario de Gobierno de la entidad.

6.7. Dispositivos

Los funcionarios y contratistas que dispongan de información en USB, Discos Duros Externos, Documentos Impresos o cualquier dispositivo de almacenamiento deberán garantizar la custodia de los mismos y no mantener en lugares de fácil acceso a terceros para evitar el acceso no autorizado a la información que en ellos se contenga.

6.8. Internet

Los empleados, funcionarios y contratistas no podrán acceder desde sus lugares de trabajo a páginas que no sean necesarias para el desarrollo de sus actividades y/o funciones tales como redes sociales, chats y plataformas.

Para evitar el acceso a sitios de internet no autorizados, el funcionario encargado realizará los bloqueos de internet y adicionalmente establecerá una política interna de acceso a internet, con el fin de lograr la accesibilidad necesaria al sistema.

6.9. Inventario tecnológico

El *Área de Sistemas* de la Secretaría de Gobierno se encargará de realizar un inventario físico de los equipos de cómputo, impresoras y demás dispositivos para establecer con que cantidad de herramientas tecnológicas cuenta la entidad y adicionalmente se hará un registro de custodia para cada uno de los funcionarios y contratistas a los que se les asigne cualquier dispositivo.

No se permitirá el acceso a dispositivos y equipos de cómputo a terceros sin previa autorización del jefe de despacho o responsable del dispositivo. El acceso a dichos dispositivos se hará siempre en presencia del funcionario o contratista responsable.

6.10. Conexiones

Las conexiones de internet a través de red WIFI se harán solo a equipos de cómputo de la entidad y para los fines pertinentes.

En caso de ser necesario, la conexión a equipos que no sean de propiedad de la entidad ésta se hará a través del responsable del Área de Sistemas adscrita a la Secretaría de Gobierno.

6.11. Antivirus

Cada equipo que sea de propiedad de la entidad y asignado a un funcionario o contratista deberá tener instalado un antivirus que se ajuste a las necesidades del equipo y que cuente con licencia.

El Área de Sistemas adscrita a la Secretaría de Gobierno, es la encargada de realizar revisiones periódicas para constatar que los equipos de cómputo cuenten con antivirus que garanticen el funcionamiento óptimo de los equipos y dispositivos.

6.12. Sistemas operativos

Los equipos que adquiera la Administración Central Municipal deberán contar con Sistemas Operativos que tengan su respectivo licenciamiento. En caso de que no contar con las licencias respectivas se utilizaran sistemas operativos de versión libre.

6.13. Aplicaciones

Los empleados, funcionarios y contratistas no están autorizados para realizar la instalación de aplicaciones con fines diferentes a las que contribuyan con la realización de sus funciones y actividades. En caso de requerir instalar cualquier aplicación, deberá solicitarlo al Área de Sistemas para que proceda con la aplicación y genere un registro.

6.14. Seguridad física de los equipos

Los empleados, funcionarios y contratistas a los que se les asigne equipo de cómputo o cualquier otro dispositivo deberán garantizar el cuidado y devolverlo en las condiciones en que los recibió.

Se realizará por parte del Área de Sistemas y previa autorización de la Secretaría de Gobierno, mantenimientos preventivos y correctivos para conservar la integridad del equipo o dispositivo.

Los empleados, funcionarios y contratistas solicitarán soporte técnico en caso de necesitarlo ante la Secretaría de Gobierno para que asigne al Área de Sistemas a realizar el respectivo soporte técnico.

6.15. Capacitaciones

La Administración Central Municipal, por intermedio de la Secretaría de Gobierno, brindará capacitación sobre seguridad y privacidad de la información y temas conexos a esta, a todos los funcionarios y contratistas con el fin de que estos estén en la capacidad de responder ante cualquier situación que se presente y garantizar la calidad, claridad y disponibilidad de la información.

6.16. Respaldo de la información

Los empleados, funcionarios y contratistas de la entidad deberán realizar copias de seguridad de la información guardada en servidores, equipos de cómputo y dispositivos de propiedad de la entidad con el fin de salvaguardar la información en caso de que de daño y/o pérdida parcial o total de esta.

7. INTERCAMBIO DE INFORMACIÓN CON ENTIDADES EXTERNAS

Las peticiones o solicitudes de información por parte de entes externos deben ser aprobadas por con la Secretaría de Gobierno y ser redireccionados a los responsables del manejo y custodia dicha información.

Tener en cuenta que la información solicitada por parte de los entes externos debe ser realizada por un medio valido que permita el registro de la solicitud, donde se pueda identificar el remitente, el asunto y la fecha aclarando que toda información institucional debe ser manejada de acuerdo a la normatividad legal vigente.

BIBLIOGRAFÍA

☑ MODELO DE IMPLEMENTACIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN -MINTIC

☑ Formato SGSI Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea 2.0