RESOLUCIÓN ADMINISTRATIVA N° 081
(Enero 27 de 2021)

POR LA CUAL SE ADOPTA EL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA ADMINISTRACIÓN MUNICIPAL DE SIBATÉ, CUNDINAMARCA.

EL ALCALDE MUNICIPAL DE SIBATÉ (CUNDINAMARCA), EN USO DE SUS FACULTADES CONSTITUCIONALES QUE TRATA EL ARTICULO 315, NUMERAL 1 Y 3; Y EN ESPECIAL DE LAS CONSAGRADAS EN LA LEY 136 DE 1994, ARTICULO 91 LITERAL D NUMERAL 1, MODIFICADA POR LA LEY 1551 DE 2012: ARTICULO 4, LEY 9 DE 1979, ARTICULO 2 RESOLUCIÓN 2400 DE 1979, ARTICULO 21, DECRETO 1295 DE 1994; LEY 1562 DE 2012; LEY DECRETO 1072 DE 2015; EN SU LIBRO 2 PARTE 2 TITULO 4 CAPITULO 6 Y

CONSIDERANDO

1. Que la Constitución Política en su artículo 113 señala que los diferentes órganos del Estado tienen funciones separadas, pero colaboran armónicamente para la realización de sus funciones.

2. Que el numeral 8 del artículo 2 de la Ley 1341 de 2009 establece que el Gobierno Nacional fijará los mecanismos y condiciones para garantizar la masificación del Gobierno en Línea (ahora Política de Gobierno Digital), con el fin de lograr la prestación de servicios eficientes a los ciudadanos, así mismo, la citada Ley determinó que es función del Estado intervenir en el sector de las TIC, con el fin de promover condiciones de seguridad del servicio al usuario final, incentivar acciones preventivas y de seguridad informática y de redes para el desarrollo de dicho sector; así como reglamentar las condiciones en que se garantizará el acceso a la información en línea, de manera abierta, ininterrumpida y actualizada.

3. Que la Ley 1712 de 2014, "por la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones", señala que sus sujetos obligados deberán observar lo establecido por la estrategia de Gobierno en Línea – (ahora Política de Gobierno Digital) en cuanto a la publicación y divulgación de información pública.

4. Que el Decreto 1078 de 2015, Por el cual se expide el Decreto Único Reglamentario del sector Tecnologías de información y las comunicaciones acoge el Decreto 1008 de 2018 subrogando lo indicado en el capítulo 1 del título 9 de la parte 2 del libro 2.

5. Que el Decreto 612 de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado, entre ellos el Plan Estratégico de Tecnologías de la Información y las Comunicaciones PETI, Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y Plan de Seguridad y Privacidad de la Información.

6. Que el Decreto 1008 de 2018, Por el cual 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".

7. Que el Artículo 2.2.9.1.2.2.del Decreto 1008 de 2018 establece que, para la implementación de la Política de Gobierno Digital, las entidades públicas deberán aplicar el Manual de Gobierno Digital que define los lineamientos, estándares y acciones a ejecutar por parte de los sujetos obligados de esta Política de Gobierno Digital, el cual será elaborado y publicado por el Ministerio de Tecnologías de la Información y las Comunicaciones, en coordinación con el Departamento Nacional de Planeación.

8. Que el Articulo 2.2.9.1.3.2. del Decreto 1008 de 2018 establece, el Responsable Institucional de la Política de Gobierno Digital. El representante legal de cada sujeto obligado, será el responsable de coordinar, hacer seguimiento y verificación de la implementación de la Política de Gobierno Digital.

9. Que el Articulo 2.2.9.1.3.3. del Decreto 1008 de 2018 establece el responsable de orientar la implementación de la Política de Gobierno Digital. Los Comités Institucionales de Gestión y Desempeño de que trata el artículo 2.2.22.3.8 del Decreto 1083 de 2015, serán los responsables de orientar la implementación de la política de Gobierno Digital, conforme a lo establecido en el Modelo Integrado de Planeación y Gestión.

10. Que el Articulo 2.2.9.1.3.4. del Decreto 1008 de 2018 establece el Responsable de liderar la implementación la Política de Gobierno Digital. El Director, Jefe de Oficina o Coordinador de Tecnologías y Sistemas de la Información y las Comunicaciones, o quien haga sus veces, de la respectiva entidad, tendrá la responsabilidad de liderar la implementación de la Política de Gobierno Digital. Las demás áreas de la respectiva entidad serán corresponsables de la implementación de la Política de Gobierno Digital en los temas de su competencia.

11. Que, dentro de los tres aspectos habilitadores transversales para la implementación de la Política de Gobierno Digital, el elemento **Seguridad de la información,** busca que las entidades públicas implementen los lineamientos de seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad y disponibilidad y privacidad de los datos. Este habilitador se soporta en el **Modelo de Seguridad y Privacidad de la Información -MSPI**, que contempla 6 niveles de madurez.

12. Que, de acuerdo con la Guía Modelo de Seguridad y Privacidad del MSPI, el Plan de tratamiento de riesgos es el 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).

RESUELVE:

ARTÍCULO PRIMERO. – ADOPCIÓN: Adóptese el Plan de tratamiento de riesgos de seguridad y privacidad de la información de la Administración Municipal de Sibaté, vigencia año 2021.

ARTÍCULO SEGUNDO. – ALCANCE E IMPLEMENTACIÓN: El Plan de tratamiento de riesgos de seguridad y privacidad de la información de la Administración Municipal de Sibaté se dicta en cumplimiento de las disposiciones legales vigentes y basada en la norma IS027001:2013, con el ánimo de gestionar adecuadamente la seguridad de la información en los procesos, en los activos, en sistemas informáticos y lógicos, partes interesada, la infraestructura de red de la organización, instalaciones físicas y el entorno.
Esta política aplica a los procesos y procedimientos de la entidad y está dirigido a todos los usuarios internos, externos, servidores, funcionarios en todas las vinculaciones.

ARTICULO TERCERO. – El Plan de tratamiento de riesgos de seguridad y privacidad de la información de la Administración Municipal de Sibaté, será actualizado teniendo en cuenta lo establecido en las exigencias normativas y/o cambio en la situación de seguridad y privacidad de la información para la entidad.

ARTÍCULO CUARTO. Articular el Plan de tratamiento de riesgos de seguridad y privacidad de la información de la Administración Municipal de Sibaté con el Plan de Acción de la Entidad.

INTRODUCCIÓN

El presente Plan de Tratamiento de Riesgos se elabora con el fin de dar a conocer como se realizará la implementación y socialización del componente de Gobierno digital en el Eje Temático de la Estrategia en **seguridad y privacidad de la información**, el cual busca proteger los datos de los ciudadanos garantizando la seguridad de la información.

1. TERMINOS 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:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (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).
- **Confidencialidad:** Propiedad que determina que la información está disponible ni sea revelada a quien no esté autorizado (2.13 ISO 27000)
- **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.

- **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).

- **Disponibilidad:** Propiedad que la información sea accesible y utilizable por solicitud de los autorizados (2.10 ISO 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).

- **Integridad:** Propiedad de salvaguardar la exactitud y el estado completo de los activos (2.36 ISO 27000)

- **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 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

- **Procedimiento**: Sucesión cronológica de acciones concatenadas entre sí, para la realización de una actividad o tarea específica dentro del ámbito de los controles de Seguridad de la Información.

- **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).

2. OBJETIVO

Mitigar los riesgos asociados a los procesos existentes de la Alcaldía Municipal de Sibaté con el fin de proteger los activos de información, el manejo de medios, el control de acceso y la gestión de los usuarios.

2.1. OBJETIVOS ESPECIFICOS

- Implementar las Políticas de la seguridad de la información
- Desarrollar un plan de trabajo para la implementación del plan de tratamiento de riesgo de seguridad y privacidad de la información.
- Aplicar las metodologías del DAPF respectivamente en seguridad y riesgo de la información.

3. RECURSOS

- **Humano:** Alcalde Municipal, Secretarios y Jefes de Oficinas, Líderes de los Proceso, Profesional de TIC.
- **Físico:** Servidores, Firewall, PC y equipos de comunicación
- **Financiero:** Plan de Adquisiciones

4. RESPONSABLES

- Alcalde Municipal
- Secretarios y Jefes de Oficina
- Líderes de los Proceso
- Profesional de TIC

5. METODOLOGÍA DE IMPLEMENTACIÓN

Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información en la Alcaldía Municipal de Sibaté, se toma referencia la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Manual de implementación versión 3.02 del Ministerio de Tecnologías de la Información y las Comunicaciones.

De acuerdo con esto, se definen las siguientes fases de implementación del MSPI:

1. **Diagnosticar**
2. **Planear**
3. **Hacer**
4. **Verificar**
5. **Actuar**

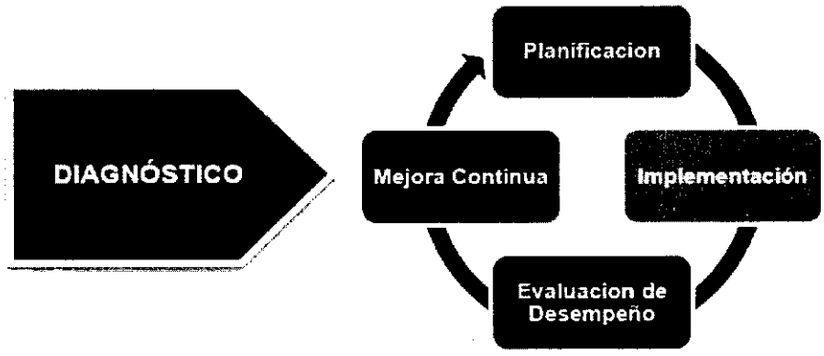

Ilustración 1Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

Fuente: Manual Modelo de seguridad y Privacidad de la Información – MINTIC

6. ACTIVIDADES PARA LA IMPLEMENTACION

1. Realizar Diagnóstico
2. Implementar políticas enfocadas a la seguridad de la Información.
3. Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información
4. Realizar Inventario de Activos de Información con los líderes de cada Proceso.
   Aclarando que se cuenta con el inventario de Activos de las bases de datos que hacen parte de la Administración Municipal

Item	Nombre sistema de información y/o aplicativo	Usuario y/o área	Nombre de los reportes que genera el sistema y/o documentos	Destinatario y/o usuario de los reportes
1	Ventaniilla única de Correspondencia Municipal	Archivo y Correspondencia	Reporte de Correspondencia recibida por terceros y planilla de distribución de correspondencia	Toda la administración Municipal de Sibaté
2	Correspondencia interna	Sec. General y de las Tic	Reporte de Correspondencia enviada y recibida	Usuarios de la secretaria general
3	Asignación de citas comisaria de familia	Comisarías de familia	Cuantificación por días y por mes la cantidad de citas asignadas en un determinado turno y con clasificaciones	Usuarios de atención a la comisaria de familia
4	PREDIAL	Área de impuestos	*Estado de cuenta para el contribuyente *Informe detallado de ingresos por punto de recaudo y fecha *Informe consolidado de ingresos por fecha *Cartera detallada por contribuyente *Cartera acumulada por vigencias	*Contribuyente de Predial *Área Financiera Profesional Universitario *Secretario de Hacienda
5	RECAUDOS	Área de impuestos	*Informe de pagos realizados por los contribuyentes *Informe detallado de ingresos por punto de recaudo y fecha *Informe consolidado de ingresos por fecha	*Contribuyente de predial *Área Financiera *Director de Tesorería e Impuestos *Secretario de Hacienda
6	CONTABILIDAD	Área Financiera	*Órdenes de pago *Comprobantes de Egreso *Certificaciones de retenciones *Resumen de cuentas movidas *Informes Mensuales (Certificado Rete fuente, Certificado Industria y Comercio, Certificado de Rete IVA, Relación de Egresos, Certificado de Ingresos y Retenciones, Relación de Estampillas, Declaración de Retención en la Fuente) *Informes anuales o auxiliar contable *Informes Ocasionales (Plan de cuentas, Documentos sin CC, Movimientos sin afectación presupuestal, Indicadores de Tesorería) *Caja Diarios *Relación de documentos presupuestales *Trazabilidad presupuestal *Informe Balance (Libro Mayor y Balance, Balance General, Estado de Resultados, Balance de	*Terceros *Área Financiera *Profesional *Secretario de Hacienda *Entes de control y vigilancia

			prueba por tercero)	
7	PRESUPUESTO	Área Financiera	*Ejecución Presupuestal *Libro Ordenador del Gasto *Relación documentos presupuestales *Resumen de pagos por rubros *Certificado de Disponibilidad Presupuestal	*Terceros *Área Financiera *Profesional Universitario *Secretario de Hacienda *Entes de control Y vigilancia
8	TESORERÍA	Área Financiera	*Libros Auxiliares Conciliaciones *Relación de Comprobantes de Ingresos - Egresos *Informe de recaudos de terceros *Informe Traslado de fondos *Informe de notas de contabilidad y bancarias	*Terceros *Área Financiera *Profesional Universitario *Secretario de Hacienda *Entes de control y vigilancia
9	COMPLEMENTARIOS	Área de impuestos	*Reporte de la liquidación emitida por las diferentes dependencias *Informe detallado por fecha de los ingresos *Informe consolidado por fecha de los ingresos	*Terceros *Entidad Financiera *Área Financiera *Profesional Universitario *Secretario de Hacienda
10	INDUSTRIA Y COMERCIO	Área de impuestos	*Estado de cuenta para el contribuyente *Informe detallado por fecha de los ingresos *Informe detallado de cartera	*Contribuyente de industria y comercio *Entidad Financiera *Área Financiera *Profesional Universitario *Secretario de Hacienda

5. Realizar la Valoración de los Activos de Información con los líderes de cada Proceso
6. Realizar el Plan de tratamiento de los riesgos (Riesgo Inherente y Riesgo Residual)
7. Socializar el Plan de Tratamiento de Riesgo
8. Realizar seguimiento del Plan de Tratamiento de Riesgo

7. CUMPLIMIENTO DE IMPLEMENTACIÓN

De acuerdo con las fases mencionadas anteriormente, se describe a continuación los dominios que se deben desarrollar y los plazos de implementación de acuerdo a lo establecido por la Alcaldía Municipal de Sibaté

- Implementar la Política de Seguridad de la información.
- Implementar la Política de Administración de datos.
- Implementar la Políticas de Comunicaciones.
- Aspectos organizativos de la seguridad de la información
- Seguridad de la Información enfocada a los recursos humanos
- Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.
- Revisión de los Controles de acceso
- Seguridad Física y del entorno
- Seguridad en las telecomunicaciones
- Gestión de Incidentes de Seguridad de la Información
- Aspectos de seguridad de la información en la gestión de continuidad del negocio.

8. CRONOGRAMA

No.	ACTIVIDAD	RESPONSABLE	FECHA DE IMPLEMENTACION
1	Realizar Diagnóstico	Profesional Universitario y/o apoyo	Septiembre de 2021
2	Implementar políticas enfocadas a la seguridad de la Información.	Profesional Universitario TICS	Octubre de 2021
3	Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información	Contratista de apoyó a las tics	Octubre de 2021
3	Realizar Inventario de Activos de Información con los líderes de cada Proceso	Líderes de proceso	Octubre de 2021
4	Realizar la Valoración de los Activos de Información con los líderes de cada Proceso	Líderes de proceso	Noviembre de 2021
5	Realizar el Plan de tratamiento de los riesgos (Riesgo Inherente y Riesgo Residual)	Contratista de apoyó a las tics	Diciembre de 2021
6	Socializar el Plan de Tratamiento de Riesgo	Contratista de apoyó a las tics	Diciembre de 2021
7	Realizar seguimiento del Plan de Tratamiento de Riesgo	Contratista de apoyó a las tics	Diciembre de 2021

9. **SEGUIMIENTO Y EVALUACIÓN**

Al finalizar cada etapa se realizará una reunión con la alta dirección, los secretarios, jefes de oficina y el equipo de trabajo para presentar el informe de avance a la implementación del PTR y de esta manera evaluar todas las actividades propuestas en dicho plan.

ARTÍCULO QUINTO. –VIGENCIA Y DEROGATORIAS: La presente Resolución, se actualiza a enero de 2021 según normatividad legal vigente y procesos de la administración Municipal y rige a partir de su publicación y deroga las disposiciones internas que le sean contrarias.

PUBLÍQUESE Y CÚMPLASE

Dado en el despacho del Alcalde Municipal de Sibaté Cundinamarca, a los veintisiete (27) días del mes de enero de dos mil veintiuno (2021).

EDSON ERASMO MONTOYA CAMARGO
ALCALDE MUNICIPAL

SERVIDOR PÚBLICO	ELABORADO	REVISADO	APROBADO
Nombres	LINDA INCIGNARES	JUAN CARLOS GUTIERREZ RAMIREZ	EDSON ERASMO MONTOYA CAMARGO
	JEFE DE PRENSA Y TICS	ecretario General	Alcalde Municipal
		Enero de 2021	