RESOLUCIÓN ADMINISTRATIVA N° 083
(Enero 27 de 2021)

POR LA CUAL SE ADOPTA EL PLAN 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, **la Política de Seguridad y Privacidad de la información** está contenida en un documento de alto nivel que incluye la voluntad de la Alta Dirección de la Entidad para apoyar la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI. La política debe contener una declaración general por parte de la administración, donde se especifique sus objetivos, alcance, nivel de cumplimiento. La política debe ser aprobada y divulgada al interior de la entidad.

RESUELVE:

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

ARTÍCULO SEGUNDO. – ALCANCE E IMPLEMENTACIÓN: El Plan 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 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 Seguridad y privacidad de la información de la Administración Municipal de Sibaté con el Plan de Acción de la Entidad.

1. POLÍTICA GENERAL DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la Administración de la Alcaldía de Sibaté 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.

La Alcaldía de Sibaté, para asegurar la dirección estratégica de la entidad, establece la compatibilidad de la política de seguridad de la información y los

objetivos de seguridad de la información, estos últimos correspondientes a:

- Minimizar el riesgo en 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 clientes de la administración municipal de la alcaldía de Sibaté.
- Garantizar la continuidad de los procesos frente a incidentes.

Alcance y aplicabilidad

- Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros de la administración municipal de la alcaldía de Sibaté.

Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

A continuación, se establecen las 12 políticas de seguridad que soportan el MSPI *(nivel de madurez en la implementación del Modelo de seguridad y Privacidad de la Información)* de la alcaldía de Sibaté:

i. La Alcaldía de Sibaté 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 de la administración, y a los requerimientos regulatorios que le aplican a su naturaleza.

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

iii. La alcaldía de Sibaté protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.

iv. La Alcaldía de Sibaté protegerá la información creada, procesada, transmitida o resguardada por sus procesos administrativos, 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.

v. La Alcaldía de Sibaté protegerá su información de las amenazas originadas por parte del personal.

vi. La alcaldía de Sibaté protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

vii. La Alcaldía de Sibaté controlará la operación de sus procesos administrativos garantizando la seguridad de los recursos tecnológicos y las redes de datos.

viii. La Alcaldía de Sibaté implementará control de acceso a la información, sistemas y recursos de red.

ix. La Alcaldía de Sibaté garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

x. La Alcaldía de Sibaté 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.

xi. La Alcaldía de Sibaté garantizará la disponibilidad de sus procesos administrativos y la continuidad de su operación basada en el impacto que pueden generar los eventos.

xii. La Alcaldía de Sibaté 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.

2. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

2.1 Justificación

La Alcaldía de Sibaté 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, ha establecido realizar un Plan de Seguridad y Privacidad de la Información con el ánimo de que no se presenten pérdidas, robos, accesos no autorizados y duplicación de la misma, igualmente promueve una política de seguridad de la información

física y digital de acuerdo a la caracterización de los usuarios tanto internos como externos.

La seguridad de la información se entiende como la preservación de las siguientes características:

a) **Confidencialidad**: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

b) **Integridad**: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

c) **Disponibilidad**: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, debe considerarse los conceptos de:

a) **Auditabilidad**: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

b) **Protección a la duplicación**: consiste en asegurar que un proceso sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe un proceso para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

c) **No repudio**: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

d) **Legalidad**: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta la administración.

e) **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.

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 de la administración, sin tener en cuenta la tecnología
utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

2.2 Objetivo

Definir los mecanismos y todas las medidas necesarias por parte de la alcaldía de Sibaté, 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.

2.3 Alcance

Este Plan de Seguridad y Privacidad de la Información y su política, son aplicables a todos los funcionarios de la Alcaldía de Sibaté, 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.

2.4 Roles y Responsabilidades

Es responsabilidad del Comité Institucional De Gestión De Desempeño de la alcaldía de Sibaté adoptado mediante Decreto 048 de 11 DE abril de 2018 con el cual se adoptó el modelo integrado de planeación y gestión – MIPG, en cumplimiento del decreto 1499 de 2017 el cual crea el comité institucional de gestión de desempeño que en su parágrafo 3° estipula "este comité sustituirá los demás comités que tengan relación con el modelo integrado de planeación y gestión y que no sean obligados por mandato legal y remplaza al Comité de Seguridad de la Información. Dicho comité está encargado de la implementación, aplicación, seguimiento y autorizaciones de la política del Plan de Seguridad y Privacidad de la información en las diferentes áreas y procesos de la entidad, además garantiza el apoyo y el uso de la Política de Seguridad de la Información como parte de su herramienta de gestión, la cual debe ser aplicada de forma obligatoria por todos los funcionarios para el cumplimiento de los objetivos.

El Comité cuya composición y funciones serán reglamentadas por una mesa de trabajo compuesta por:

- Secretario general
- Secretaría de planeación
- Oficina Control Interno
- Oficina TIC - Prensa

Este comité deberá revisar y actualizar esta política anualmente presentando las propuestas a la alta dirección para su aprobación.

2.5 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, la alcaldía de Sibaté se reserva el derecho de tomar las medidas correspondientes.

2.6 Comunicación

Mediante socialización a todos los funcionarios de la alcaldía de Sibaté 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.sibate-cundinamarca.gov.co.

2.7 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.

DESCRIPCIÓN DE LAS POLITICAS

3. Generalidades

La Alcaldía de Sibaté 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.

3.1 Gestión de Activos

3.1.1 Política para la identificación, clasificación y control de activos de información

La Alcaldía de Sibaté 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 facilitador del proceso de Gestión de Recursos Físicos con apoyo del técnico operativo de sistemas tiene la responsabilidad de mantener el inventario completo y actualizado de los recursos de hardware y software de la entidad.

Aspectos a 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 la Alcaldía de Sibaté 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 o saquen copias: verificar las áreas adyacentes a impresoras, escáner y fotocopiadoras para asegurarse que no quedaron documentos relacionados o adicionales; asimismo, recoger de las impresoras, escáner y fotocopiadoras, 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 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. 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.

3.2 Control de Acceso

3.2.1 Política de acceso a redes y recursos de red

El funcionario encargado TIC´s de la Alcaldía de Sibaté, 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.

Aspectos a tener en cuenta:

a) El proceso Gestión de TIC debe asegurar que las redes inalámbricas de la alcaldía de Sibaté 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 la Alcaldía de Sibaté, 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 la Alcaldía de Sibaté, 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 la Alcaldía de Sibaté deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

3.2.2 Política de administración de acceso de usuarios

La Alcaldía de Sibaté 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.

Aspectos a tener en cuenta:

a) El proceso Gestión de TIC's, debe definir lineamientos para la configuración de contraseñas que aplicarán sobre la plataforma tecnológica, los servicios de red y los sistemas de información de la Alcaldía de Sibaté; 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.

3.2.3 Política de control de acceso a sistemas de información y aplicativos

La Alcaldía de Sibaté 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.

Aspectos a 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 la Alcaldía de Sibaté.
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 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.
g) 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

3.2.4 Políticas de seguridad física

La Alcaldía de Sibaté 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 el cuarto de comunicaciones.

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

Aspectos a 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 alcalde 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.

d) El alcalde 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 la alcaldía de Sibaté.

e) Los ingresos y egresos de personal a las instalaciones de la alcaldía de Sibaté 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) El funcionario debe portar el carné que los identifica como tal en un lugar visible mientras se encuentren en las instalaciones de la alcaldía de Sibaté; 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.

3.2.5 Política de seguridad para los equipos

La alcaldía de Sibaté 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.

Aspectos a 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 la alcaldía de Sibaté.

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.

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.

d) 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.

e) 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.

f) 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 la alcaldía de Sibaté cuente con la autorización documentada y aprobada previamente por el área.

g) 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.

h) 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 la Alcaldía de Sibaté.

i) 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.

j) Cuando se presente una falla o problema de hardware o software u otro recurso tecnológico propiedad de la Alcaldía de Sibaté, 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.

k) 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.

l) Los equipos de cómputo, bajo ninguna circunstancia, deben ser dejados desatendidos en lugares públicos o a la vista, en el caso de que estén siendo transportados.

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

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

o) 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.

p) 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.

3.2.6 Política de uso adecuado de internet

La Alcaldía de Sibaté 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

Aspectos a 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 la alcaldía de Sibaté 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, hacking y/o cualquier otra página que vaya en contra de la ética moral, bioética y leyes vigentes o políticas establecidas en este documento.

i) Los usuarios del servicio de internet tendrán un horario limitado para el uso de redes sociales u otro tipo de servicio que tengan como objetivo crear comunidades para interactuar y/o intercambiar información, Con esto se garantizan el correcto desarrollo de las actividades propias de la Alcaldía de Sibaté.

j) No está permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, fotos personales, 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 la alcaldía de Sibaté, de los funcionarios, con terceros.

4. PRIVACIDAD Y CONFIDENCIALIDAD

4.1 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, la alcaldía de Sibaté a través del Comité, 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 la alcaldía de Sibaté, 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, hayan suministrado datos personales. En caso de delegar a un tercero el tratamiento de datos personales, la alcaldía de Sibaté 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.

Aspectos a 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.

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.

e) El comité debe establecer los controles para el tratamiento y protección de los datos personales de los beneficiarios, funcionarios, proveedores y demás terceros de la alcaldía de Sibaté 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 la alcaldía de Sibaté 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.

4.2 Disponibilidad del servicio e información

La alcaldía de Sibaté 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.

4.2.1 Política de continuidad, contingencia y recuperación de la información

La Alcaldía de Sibaté 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 la Alcaldía de Sibaté 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 administrar 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.

Aspectos a tener en cuenta:

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.

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 PUBLICO	ELABORADO	REVISADO	APROBADO
Nombres	LINDA INCIGNARES	JUAN CARLOS GUTIERREZ RAMIREZ	EDSON ERASMO MONTOYA CAMARGO
Cargo	JEFE DE PRENSA Y TICS	Secretario General	Alcalde Municipal
Fecha	Enero de 2021		