ALCALDÍA MUNICIPAL DEL LÍBANO

POLÍTICA DE SEGURIDAD DIGITAL

Octubre 2023

TABLA DE CONTENIDO

	INTRODUCCIÓN	3
1.	PRESENTACIÓN	4
2.	OBJETIVOS	4
2.1.	Objetivo general	4
2.1.	Objetivos Específicos	4
3.	ALCANCE	5
4.	RESPONSABLE	5
5.	MARCO JURIDICO Y LEGAL	5
6.	DIAGNOSTICO DE LA POLITICA	7
7.	DEFINICIÓN DE LA POLÍTICA	7
7.1.	Plan de Acción para la Implementación de la Política	8
8.	LINEAMIENTOS GENERALES DE LA POLITICA	8
9.	POLITICAS DE PRIVACIDAD Y CONFIDENCIALIDAD	10
9.1	Política de Tratamiento de Datos Personales	10
10.	SEGUIMIENTO Y MEDICIÓN DE LA POLÍTICA	12
11.	CONCEPTOS Y DEFINICIONES	12
12.	BIBLIOGRAFIA	14

INTRODUCCIÓN

El Modelo Integrado de Planeación y Gestión MIPG es un marco de referencia paradirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de lasentidades y organismos públicos, con el fin de generar resultados que atiendan losplanes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, conintegridad y calidad en el servicio.

La puesta en marcha del Modelo Integrado de Planeación y GestiónMIPG, busca mejorar la capacidad del Estado para cumplirle a la ciudadanía,incrementando la confianza de ésta en sus entidades y en los servidorespúblicos, para lograr mejores niveles de gobernabilidad y legitimidad que redundarán como primera medida en la generación de resultados con valores, mejor coordinacióninterinstitucional, mayor compromiso del servidor público, aprovechamiento y difusión de información confiable y oportuna.

La Política Nacional de Seguridad Digital con base en Documento CONPES 3854 de 2016, orienta y suministra los lineamientos para ser ejecutada por las entidades públicas, en la identificación, gestión, tratamiento y mitigación de los riesgos de seguridad digital en las actividades socioeconómicas en el entorno digital, para contribuir al crecimiento de la economíaa través de la tecnología de la información, así como para la toma de decisiones de la Administración Municipal basada en evidencias de información que se genera, almacena y administra, por lo que es vital establecer políticas claras y contundentes.

La tecnología es el recurso vital para el manejo de la información, la cual se desarrolla, crece y evoluciona de manera rápida y constante, requiriendo lineamientos de seguridad que minimicen las alteración, fuga o indisponibilidad de la información durante las etapas de elaboración, diseño e implementación de las herramientas, incluso durante el uso de las mismas. Es así como la política de seguridad de la información debe definir lineamientos, controles, roles perfiles y responsabilidades para la gestión de la información, gestionar al máximo las amenazas a los sistemas de información, control y gestión y limitar la capacidad de los atacantes para violentar y dar un mal uso a la información.

1. PRESENTACIÓN

La Administración Municipal del Líbano, en su empeño por mejorarla infraestructura de tecnología de información y comunicación (TIC), establece lineamientos y estándares que permitirán el desarrollo de los componentes y los propósitos de la política de Gobierno Digital como es la seguridad de la Información, que preservará la confidencialidad, integridad y disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos.

Esta política complementa lo expuesto en la Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas, emitida conjuntamente entre el Departamento Administrativo de la Función Pública y la Secretaría de Transparencia de la Presidencia de la República, específicamente en las secciones de Análisis del contexto (con un enfoque hacia el entorno digital), identificación de activos, catálogos de amenazas y vulnerabilidades para el análisis de riesgos de seguridad digital, controles para la mitigación de los riesgos de seguridad digital, el reporte de riesgos de seguridad digital y otros aspectos adicionales para llevar a cabo una gestión del riesgo de seguridad digital adecuada.

La declaración de laPolítica de Seguridad de la Información Institucional, busca proteger los activos de información (grupos de valor, información, procesos, tecnologías de información incluido el hardware y el software), a través de los lineamientos y directrices para la implementar la seguridad de la información en la gestión de los procesos internos, bajo el marco del Modelo Integrado de Planeación y Gestión.

2. OBJETIVOS

2.1 Objetivo General

Definir las estrategias, mecanismos y usos de las tecnologías de la información y las comunicaciones, mediante los cuales se desarrollará e implementará la Política de Seguridad Digital, con el fin de proteger los activos de información en los procesos para la construcción de una Administración más participativa, eficiente y transparente, aplicando buenas prácticas del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno Digital.

2.2 Objetivos Específicos

- Identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en las actividades de la Alcaldía, con servidores capacitados y sensibilizados sobre el tema.

- Desarrollar los documentos y herramientas que tiene a disposición el Min TIC, junto con el Modelo de Seguridad y Privacidad de la Información y el compendio de las normas técnicas colombianas NTC ISO/IEC 27000.

- Revisar y aprobar los activos y riegos de Seguridad Digital.

- Salvaguardar los activos tecnológicos y custodiar la información digital producida en la Entidad.

- Realizar campañas de concientización en temas de Seguridad Digital a los servidores de la Entidad, ciudadanía y partes interesadas.

- Adquirir dispositivos que permitan proteger la información digital de la Institución.

3. ALCANCE

La presente política aplica en el desarrollo en todos los procesos y a todos los servidores de la Entidad que procesan y manejan información incluida la recopilación, análisis, procesamiento, disponibilidad, custodia, conservación y recuperación y deben preservar la confidencialidad de la información que por razones de su cargo o responsabilidades designada esté bajo su custodia.

4. RESPONSABLE

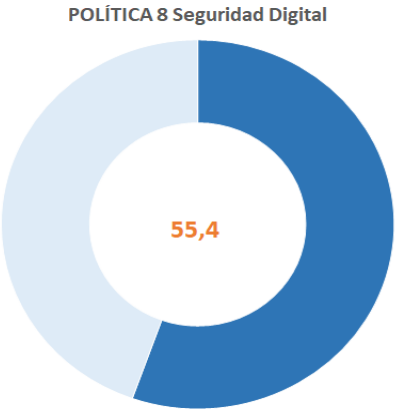
El Comité Institucional de Gestión y Desempeño de la Alcaldía Municipal del Líbano, designó al Coordinador de las TICS como responsable de la implementación de la política con el propósito de articular los esfuerzos, recursos, metodologías y estrategias para asegurar su implementación

5. MARCO JURÍDICO Y LEGAL

NORMATIVA	EPÍGRAFE
Ley 1273 de 2009	Por medio de la cual se 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, entre otras disposiciones.
Ley Estatutaria 1581 del 2012	Por la cual se dictan disposiciones generales para la Protección de Datos Personales.
Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Ley 1928 de 2018	Por medio de la cual se aprueba el "Convenio sobre la ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest
Decreto 2364 de 2012	Por medio del cual se reglamenta el artículo 7° de la ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.
Decreto 2693 de 2012	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.
Decreto 103 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones
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.
Acuerdo 03 de 2015 del AGN	Por el cual se establecen lineamientos generales para las entidades del Estado en cuanto a la gestión de documentos electrónicos generados como resultado del uso de medios electrónicos de conformidad con lo establecido en el capítulo IV de la Ley 1437 de 2011, se reglamenta el artículo 21 de la Ley 594 de 2000 y el capítulo IV del Decreto 2609 de 2012
Conpes 3854 de 2016	Política Nacional de Seguridad Digital

6. DIAGNÓSTICO DE LA POLÍTICA

El diagnóstico de la Política se realiza a través de los resultados del FURAG reportados en la presente vigencia y que corresponden a la evaluación del año 2022, encontrando un puntaje de **55,4**, calificación que puede mejorar instaurando los lineamientos que emite MINTIC, para desarrollar las herramientas y mecanismos para su mejora.



Fuente: Función pública Resultados FURAG

7. DEFINICIÓN DE LA POLÍTICA

"La Alcaldía Municipal del Líbano, se compromete a implementar y garantizar la confidencialidad, integridad y disponibilidad de la información que maneja y a otorgar los recursos necesarios para administrar los riesgos de Seguridad Digital, con el propósito de brindar confianza a la ciudadanía, grupos de valor y partes interesadas, además cumplir con todos los requisitos, legales, reglamentarios,contractuales y establecer reglas, y directrices orientadas proteger los activos de información, de una manera eficiente y efectiva".

La implementación de la política se hará a través de la adopción e implementación del Modelo de Gestión de Riesgosde Seguridad Digital dispuesto por la Alcaldía.

7.1 Plan de Acción para la Implementación de la Política

Categoría De política	Estrategia	Actividades de Gestión	Dependencia Responsable	Periodicidad
Gestión de Servicios TIC	Aplicar el Modelo de Seguridad y Privacidad de la Información – MSPI.	Diseñar, definir o actualizar los documentos y controles del Sistema de Gestión de Seguridad de la Información.	Oficina TIC	Anual
		Formular o actualizar Plan de Seguridad y Privacidad de la Información.		Permanente
	Contar con el Plan de activos deinformación de la Alcaldía	Diseñar, definir o actualizarel inventario de activos de información.		Permanente
	Plan de riesgos de Seguridad Digital de la Alcaldía.	Diseñar, definir o actualizar la gestión de los riegos de seguridad digital de la Entidad.		Anual

8. LINEAMIENTOS GENERALES DE LA POLITICA

- Todos los servidores públicos, contratistas y demás colaboradores vinculados a la Entidad, deben velar por la seguridad y la calidad de la información en los criterios de confidencialidad, integridad, disponibilidad, efectividad, eficiencia, confiabilidad y cumplimiento y aplicar tanto la política como los controles de seguridad de la información definidos para preservar la confidencialidad de los activos de información institucionales.

- Seprohíbe realizar cambios a los activos de información de la Alcaldía, sin contar con la autorización formal del responsable del activo y/outilizar los activos de información de la entidad para fines diferentes al cumplimiento de las funciones asignadas.

- El Coordinador de TICS encargado de Seguridad de la Información, esel responsable de realizar las consultas para la identificación de comportamientos.

- Toda la información que se genere, procese, almacene, transfiera o transmita la Alcaldía en medios físicos o digitales, en sus servicios tecnológicos, infraestructura tecnológica o activos de información es de su propiedad y solo puede ser utilizada para el cumplimiento de las funciones institucionales.

- La Alcaldía Municipalserá responsable del tratamiento de los datos personales y hará uso de ellos únicamente para las finalidades que se facultan, según lo establece en su política institucional de tratamiento de datos personales.

- Todos los activos de información deben estar inventariados y deben de tener un responsable, para su custodia y tener definidas y actualizadas las restricciones de acceso.

- Los propietarios de los activos de información son responsables de su uso y protección mientras estén en su custodia en medio físico o electrónico y de informar a los jefes inmediatos de cualquier incidente de seguridad que se pueda presentar, tales como: uso indebido, alteración y/o divulgación no autorizados.

- Los activos de información tanto de manera digital y física deben seguir los lineamientos para la organización de documentos asociados al proceso de Gestión Documental, en todos los aspectos relacionados con la organización, manejo, control y servicios de los documentos que producen cada una de las dependencias en el cumplimiento de sus funciones.

- Los responsables de los activos de información deben seguir los lineamientos del Plan Institucional de Archivos – PINAR de la Alcaldía Municipal del Líbano, como instrumento de planeación para la labor archivística, que determina elementos importantes para la Planeación Estratégica y Anual del Proceso de Gestión Documental y da cumplimiento a las directrices del Archivo General de la Nación y a la normatividad vigente para la administración de los documentos..

- La Alcaldía, verificará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

- Toda información que provenga de un archivo externo de la Entidad o que deba ser descargada tiene que ser analizado con el antivirus institucional vigente.

- Ningún colaboradorque use los medios digitales de la institución, debe visitar sitios restringidos de manera explícita o implícita, o sitios que afecten la productividad de la Entidad. o a sitios relacionados con pornografía, juegos, redes sociales no autorizadas, etc.

- Cada funcionario de la Administración Municipal, tendrá un usuario con contraseña personal e intransferible de los aplicativos, correo electrónico, plataformas institucionales y demás para el desempeño de sus funciones.

- No deben descargarse juegos ni aplicativos en ninguno de los equipos de la administración.

- El uso e información de cada equipo es responsabilidad del funcionario asignado. Lineamientos para medios removibles.

- Son medios removibles todos aquellos dispositivos electrónicos que almacenen información y pueden ser extraídos de los computadores, para lo cual se establecen los siguientes lineamientos:

  - El servicio de acceso a internet, sistema de información, medio de almacenamiento, aplicaciones (Software), cuentas de red, navegadores y equipos de cómputo son propiedad de la Alcaldía y deben ser usados únicamente para el cumplimiento de la misión de la entidad.

  - El manejo, configuración, y actualización de la página institucional es exclusivamente de la Oficina TICS o del personal que delegue la Secretaria de Gobierno para tal fin.

  - Los usuarios deben tratar los mensajes de correo electrónico, chat y archivos adjuntos como información de propiedad de la Alcaldía.

  - Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.

  - Los usuarios internos de la Entidad, podrán enviar información reservada y/o confidencial vía correo electrónico siempre y cuando vayan de manera encriptado y destinada exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones.

9. POLITICAS DE PRIVACIDAD Y CONFIDENCIALIDAD

9.1 Política de Tratamiento de Datos Personales

Los datos personales que los ciudadanos, usuarios, servidores públicos y proveedores suministran al Municipio del Líbano, en cualquiera de sus procesos, serán utilizados para la prestación del servicio solicitado y serán incorporados en una base de datos cuya responsabilidad y manejo está a cargo del Municipio, serán administrados de forma confidencial con las garantías institucionales, legales y demás normas aplicables a la protección de datos personales.

- La Alcaldía del Líbano, transferirá la información a un tercero únicamente si está obligado a hacerlo por orden de autoridad administrativa o judicial.

- La alcaldía del Líbano se abstiene de ceder, vender o compartir los datos de carácter personal recolectados, sin la expresa autorización del usuario.

- No responderá en ningún caso y bajo ninguna circunstancia, por los ataques o incidentes contra la seguridad de su sitio web o contra sus sistemas de información; o por cualquier exposición o acceso no

autorizado, fraudulento o ilícito a su sitio web y que afecten la confidencialidad, integridad o autenticidad de la información publicada o asociada con los contenidos y servicios que se ofrecen en él.

- **El Tratamiento de los datos s**e realizara para:

  - La vinculación, desempeño de funciones o prestación de servicios, retiro o terminación de contrato.
  - Para seguridad de las personas, los bienes e instalaciones de gobierno.
  - Para los fines relacionados con el desarrollo el proceso de gestión contractual de productos o servicios que la entidad requiera para su funcionamiento de acuerdo a la normatividad vigente.

- **Derecho de los Titulares**

  - Conocer, actualizar y rectificar sus datos personales frente al responsable y encargado del tratamiento. Este derecho se podrá ejercer entre otros ante datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente o se exceptúe como requisito para el tratamiento, de conformidad con lo previsto en el artículo 10 de la ley 1581 de 2012.
  - Ser informado por el Municipio como responsable del tratamiento y encargado del tratamiento, previa solicitud, respecto del uso que les ha dado a los datos personales del Titular.
  - Presentar ante el municipio quejas por infracciones a lo dispuesto en la ley 1581 de 2012 y las demás normas que la modifiquen
  - Revocar la autorización y/o solicitar la supresión del dato personal cuando en el tratamiento no se respeten los principios derechos y garantías constitucionales legales.
  - La revocatoria y/o supresión procederá cuando el Municipio haya determinado que en el tratamiento el responsable o encargado han incurrido en conductas contrarias a la Ley 1581 de 2012 y la Constitución.

- **Autorización del Titular**

Sin perjuicio de las excepciones previstas en la ley, en el tratamiento se requiere la autorización previa expresa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta y verificación posterior.

La autorización del Titular no será necesaria cuando se trate de:

- Información requerida por el Municipio en ejercicio de sus funciones legales o por orden judicial.

- **Datos de naturaleza pública**

  - Casos de urgencia médica o sanitaria.
  - Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
  - Datos relacionados con el Registro Civil de las Personas.

- **Acuerdo de Confidencialidad**

Implica que la información conocida por todo funcionario, contratista y/o tercero, bajo ninguna circunstancia deberá ser revelada por ningún medio electrónico, verbal, escrito u otro, ni total, ni parcialmente, sin contar con previa autorización.

- **Seguridad de Computadores y Portátiles**

Para lograr un alto rendimiento y salvaguarda de computadores y portátiles, la administración municipal ha definido los siguientes parámetros.

- Los computadores de mesa, portátiles, y cualquier activo de tecnología de información, podrán salir de las instalaciones únicamente con la aprobación del jefe de la dependencia.
- El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones de la Alcaldía del Líbano.
- Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del computador.
- Los usuarios deberán asegurarse de respaldar la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo, para prevenir la perdida involuntaria de información, derivada del proceso de reparación.
- Los equipos de la Alcaldía solo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.
- Debe respetarse y no modificar la configuración de hardware y software establecida por la oficina TICS.
- Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente a las oficinas de las TIC y poner el computador en cuarentena hasta que el problema sea resuelto.
- No debe utilizarse software descargado de internet y en general software que provenga de una fuente no confiable, a menos que haya sido

comprobado de una forma rigorosa y que esté aprobado su uso por la Oficina TICS de la Alcaldía.

- Para prevenir demandas legales o la introducción de virus informáticos, se Prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario.
- El personal que utiliza un computador portátil que contenga información confidencial de la institución, no debe dejarlo desentendido sobre todo cuando este de viaje.

10.SEGUIMIENTO Y MEDICIÓN DE LA POLÍTICA

La Política de Seguridad Digital se debe revisar y actualizar anualmente para garantizar la vigencia con las actualizaciones que se surten ordinariamente y cuando se realicen cambios organizacionales, culturales, operativos, cuando ocurran incidentes con respecto a los riesgos., el seguimiento se debe realizar también anualmente.

11. CONCEPTOS Y DEFINICIONES

Activo de Información: En relación con la privacidad de la información, serefiere al activo que contiene información pública que el sujeto obligado genere,obtenga, adquiera, transforme o controle en su calidad de tal.

Amenazas: Causa potencial de un incidente no deseado, que puede provocardaños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo ydeterminar el nivel de riesgo. (ISO/IEC 27000).

Lineamientos: Directriz o disposición establecida por el Ministerio TIC, que debeser implementada por las entidades públicas para el desarrollo de la Política deGobierno Digital y se desarrolla a través de estándares, guías, recomendaciones obuenas prácticas.

Estándar: Es el conjunto de características y requisitos que se toman comoreferencia o modelo y son de uso repetitivo y uniforme. Un estándar se construye através de consenso y refleja la experiencia y las mejores prácticas en un área enparticular, implican uniformidad y normalización y es de obligatorio cumplimiento.

Seguridad de la Información: Este habilitador busca que las entidadespúblicas incorporen la seguridad de la información en todos sus procesos, trámites,servicios, sistemas de información, infraestructura y en general, en todos los activosde información con el fin de preservar la confidencialidad, integridad, disponibilidad,y privacidad de la información, así como la protección de los datos personales quetratan las entidades públicas en cumplimiento de la normatividad de protección dedatos personales; este habilitador tiene su soporte en el MSPI.

12. BIBLIOGRAFÍA

- Manual Operativo del Modelo Integrado de Planeación y Gestión, 2021 V4.
- Guía de Implementación de la Política de Seguridad Digital Ministerio de Educación Nacional.
- Política de Seguridad de la Información DAFP. Versión 04 Febrero 2020.
- Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas 2018.

CONTROL DE ACTUALIZACIONES.

Versión	Fecha de Aprobación	Descripción del Cambio
01	Noviembre de 2021	Creación
02	Octubre 2022	Actualización del autodiagnóstico y el resultado FURAG
03	Octubre 2023	Actualización del documento con cambios en la definición de la Política, Plan de Acción y en el Autodiagnóstico institucional.

Elaborado por:	Revisado por:	Aprobado por:
Grupo de Planeación y TICS	Secretario de Planeación Municipal	Comité de Gestión y Desempeño Institucional