DECRETO N°
(135)

"POR EL CUAL SE ADOPTA LA POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA ALCALDÍA MUNICIPAL DE SOPÓ Y SE DEROGA LA RESOLUCIÓN N°2838 DE 2018"

En uso de sus facultades legales y constitucionales, en especial las conferidas en el artículo 91 de la ley 136 de 1994, modificada por el artículo 29 de la Ley 1551 de 2012, la Ley 1270 de 2009, la Ley 1341 de 2009, Ley 1581 de 2012, el Decreto Nacional 2573 de 2014, el Decreto 1377 de 2013, el Decreto 1008 de 2018, Decreto No 110 de 2021 y demás normas concordantes y

CONSIDERANDO

Que el artículo 2 de la Constitución Política establece *"Son fines esenciales del Estado: servir a la comunidad, promover la prosperidad general y garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución; facilitar la participación de todos en las decisiones que los afectan y en la vida económica, política, administrativa y cultural de la Nación; defender la independencia nacional, mantener la integridad territorial y asegurar la convivencia pacífica y la vigencia de un orden justo".*

Que la Constitución Política de Colombia establece en su Artículo 15 *"Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas".*

Que el Artículo 209 de la Constitución Política de Colombia consagra que *"la función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad, mediante la descentralización, la delegación y la desconcentración de funciones. Las autoridades administrativas deben coordinar sus actuaciones para el adecuado cumplimiento de los fines del Estado. La administración pública, en todos sus órdenes, tendrá un control interno que se ejercerá en los términos que señale la ley".*

Que el numeral 3° del artículo 315 de la Constitución Política prevé que corresponde al Alcalde: *"Dirigir la acción administrativa del municipio; asegurar el cumplimiento de las funciones y la prestación de los servicios a su cargo; representarlo judicial y extrajudicialmente; y nombrar y remover a los funcionarios bajo su dependencia y a los gerentes o directores de los establecimientos públicos y las empresas industriales o comerciales de carácter local, de acuerdo con las disposiciones pertinentes.*

Que el numeral 1° contenido en el literal d) del artículo 91 de la Ley 136 de 1994 modificado por el artículo 29 de la Ley 1551 de 2012, indica dentro de las funciones del Alcalde Municipal *"Dirigir la acción administrativa del municipio; asegurar el cumplimiento de las funciones y de la prestación de los servicios a su cargo; representarlo judicial y extrajudicialmente".*

Que la Ley 1273 de 2009, 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.*

DECRETO N°
(-- 135)

Que la Ley 1341 de 2009, determina el marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones, su ordenamiento general, el régimen de competencia, la protección al usuario, así como lo concerniente a la cobertura, la calidad del servicio, la promoción de la inversión en el sector y el desarrollo de estas tecnologías, el uso eficiente de las redes y del espectro radioeléctrico, así como las potestades del Estado en relación con la planeación, la gestión, la administración adecuada y eficiente de los recursos, regulación, control y vigilancia del mismo y facilitando el libre acceso y sin discriminación de los habitantes del territorio nacional a la sociedad de la información.

Que la Ley 1581 de 2012 establece en su artículo 1 que su objeto es *"desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política".*

Que el Decreto Nacional 2573 de 2014 define en su artículo 1 que *"los lineamientos, plazos y términos para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el fin de contribuir con la construcción de un Estado más eficiente, más transparente y participativo y que preste mejores servicios con la colaboración de toda la sociedad".*

Que la Ley 1581 de 2012 que expidió el Régimen General de Protección de Datos Personales, en su artículo 1°, tiene por objeto *"(...) desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma*

Que el Modelo de Seguridad y Privacidad de la Información, establece instructivos y lineamientos respecto de la implementación de este modelo y de sus lineamientos a todas las entidades nacionales y territoriales con el fin de minimizar los incidentes de seguridad digital a través de la implementación de controles de seguridad físicos y lógicos.

Que el Decreto 1008 de 2018, en su artículo 2.2.9.1.1.3 establece que como principios de la política de gobierno digital el de *"(...)**Seguridad de la Información:** Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano".*

Que mediante el Decreto No 110 de 2021 se conforma el Comité de Seguridad de la Información al interior de la Alcaldía Municipal de Sopó.

Que es necesario determinar los lineamientos que permitan proteger la Información de **LA ALCALDÍA MUNICIPAL DE SOPÓ** a través de acciones de aseguramiento de la Información teniendo en cuenta los requisitos legales, operativos, tecnológicos, de seguridad de la entidad alineados con el contexto de direccionamiento estratégico y de gestión del riesgo con el fin de asegurar el

DECRETO N°
(135)

cumplimiento de la integridad, disponibilidad, legalidad y confidencialidad de la información.

Que con base al modelo de Seguridad y privacidad de la información del Ministerio de Tecnologías de la Información y las Comunicaciones la Administración Municipal debe realizar un Manual de políticas, donde se describan los objetivos, alcances y el nivel de cumplimiento, que garanticen el adecuado uso de los activos de información al interior de la Entidad; definiendo las responsabilidades generales y específicas para la gestión de la seguridad de la información.

En mérito de lo expuesto, el Alcalde municipal de Sopó,

DECRETA

ARTÍCULO PRIMERO: **ADOPTAR** la Política General de Seguridad y Privacidad de la Información, la cual hace parte integral del presente acto administrativo.

ARTÍCULO SEGUNDO: Realizar la Socialización de las Políticas Generales de seguridad y privacidad de la información de la Alcaldía Municipal de Sopó.

ARTÍCULO TERCERO: REMITIR copia del presente Decreto a la Secretaría de Desarrollo institucional.

ARTÍCULO CUARTO. PUBLICAR el presente Decreto en la página Web de la Alcaldía Municipal de Sopó.

ARTÍCULO QUINTO. El presente Decreto rige a partir de su expedición y deroga las demás disposiciones que le sean contrarias, en especial Resolución N° 2838 de 2018 *"Por medio de la cual se adopta la Política General de seguridad y privacidad de la información de la Alcaldía Municipal de Sopó.*

COMUNÍQUESE Y CÚMPLASE

Dado en el Municipio de Sopó, Cundinamarca, el 05 AGO 2021

MIGUEL ALEJANDRO RICO SUÁREZ
Alcalde Municipal de Sopó

Aprobó: Daniel Alejandro Marín Valencia – Jefe de la Oficina Asesora Jurídica y de Contratación.
Revisó: Daniel Antonio Ayala Mora – Alala Juris Estudio Jurídico – Asesor jurídico del Despacho.
Revisó: Javier Eduardo Jiménez Forero – Jefe Oficina Asesora de Planeación Estratégica.
Revisó: Segundo Sanabria Alarcón – Secretario de Desarrollo Institucional.
Revisó: Óscar Javier Peña Muñoz – Asesor jurídico externo.
Revisó: Diego Fabián León Beltrán – Profesional Universitario.
Proyectó: Juan Carlos Rodríguez Camargo – Contratista Gobierno Digital.

DECRETO N°
(135)

SECRETARÍA DE DESARROLLO INSTITUCIONAL
ALCALDÍA MUNICIPAL DE SOPÓ
CUNDINAMARCA - COLOMBIA
2021

POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Miguel Alejandro Rico Suárez
Alcalde Municipal

Segundo Hipólito Sanabria Alarcón
Secretario de Desarrollo Institucional

Diego Fabián León Beltrán
Profesional Universitario Área de Sistemas de Información

Juan Carlos Rodríguez Camargo
Contratista Gobierno Digital

DECRETO N°
(- - 135)

POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. OBJETIVOS

1.1. OBJETIVO GENERAL

Determinar los lineamientos que permitan proteger la Información de **LA ALCALDÍA MUNICIPAL DE SOPÓ** a través de acciones de aseguramiento de la Información teniendo en cuenta los requisitos legales, operativos, tecnológicos, de seguridad de la entidad alineados con el contexto de direccionamiento estratégico y de gestión del riesgo con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad y legalidad de la información.

1.2. OBJETIVOS ESPECÍFICOS

LA ALCALDÍA MUNICIPAL DE SOPÓ, para el cumplimiento de su misión, visión, objetivos estratégicos, establece la función de Seguridad de la Información en la Entidad, con el objetivo de:

- Mantener la confianza de los ciudadanos en general y el compromiso de todos los funcionarios, contratistas o practicantes de la entidad respecto al correcto manejo y protección de la información que es gestionada y resguardada en **LA ALCALDÍA MUNICIPAL DE SOPÓ**.
- Identificar e implementar las tecnologías necesarias para fortalecer la función de la seguridad de la información.
- Implementar el Sistema de Gestión de Seguridad de la Información.
- Proteger la información y los activos tecnológicos de la Entidad.
- Asegurar la identificación y gestión de los riesgos a los cuales se exponen los activos de información de la entidad.
- Cumplir con los principios de seguridad de la información: confidencialidad, integridad y disponibilidad.
- Atender las necesidades para el cumplimiento de la función administrativa.
- Proteger la información y los activos tecnológicos de la Entidad.
- Concientizar a la alta dirección, funcionarios, contratistas y practicantes de la Entidad 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 integridad y disponibilidad de la información.

- Dar cumplimiento a los lineamientos establecidos en la Estrategia de Gobierno Digital respecto al Marco de Seguridad y Privacidad de la Información (MSPI).

2. ALCANCE

- La Política de Seguridad de la Información aplica a toda la Entidad, sus funcionarios, contratistas y practicantes de **LA ALCALDÍA MUNICIPAL DE SOPÓ**, que tengan acceso a información a través de los documentos, equipos de cómputo, infraestructura tecnológica y canales de comunicación de la entidad. Lo anterior, de conformidad a la normatividad colombiana vigente aplicable ya sea de carácter Internacional, Nacional, Departamental y/o municipal.

3. DEFINICIONES

ACEPTACIÓN DEL RIESGO: Decisión de asumir un riesgo.

ACTIVOS: 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.

AMENAZA: Se puede definir como amenaza a todo elemento o acción capaz de atentar contra la seguridad de la información.

ANÁLISIS DE RIESGO: Es un proceso que comprende la identificación de activos de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para tratar el riesgo.

ANTIVIRUS: Es una categoría de software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus. El antivirus debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

BACKUP (COPIA DE SEGURIDAD): Copia de seguridad que se realiza sobre ficheros o aplicaciones contenidas en un ordenador con la finalidad de recuperar los datos en el caso de que el sistema de información sufra daños o pérdidas accidentales de los datos almacenados. Los dispositivos más empleados para llevar a cabo la técnica de backup pueden ser discos duros, discos ópticos, USB o DVD. También es común la realización de copias de seguridad mediante servicios de copia basados en la nube. Es de suma importancia mantener actualizada la copia de seguridad, así como tener la máxima diligencia de su resguardo, para evitar pérdidas de información que pueden llegar a ser vitales para el funcionamiento ya sea de una empresa, institución o de un contenido de tipo personal. Además, cada cierto tiempo es conveniente comprobar que la copia de seguridad puede restaurarse con garantías.

CAUSA: Es el motivo por el cual sucede algo.

DECRETO N°
(135)

CIBERSEGURIDAD: La ciberseguridad es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos.

CONFIDENCIALIDAD: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

CONTROL DE ACCESO: Permitir o inhabilitar a alguien para acceder a las aplicaciones o servicios de la red a través de conexiones remotas.

DECLARACIÓN DE APLICABILIDAD: Documento que describe los objetivos de control y los controles pertinentes y aplicables para el SGSI de la organización.

DISPONIBILIDAD: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

ENTIDADES PUBLICAS: Entidad pública de carácter nacional del nivel superior ejecutivo central, que coordina la política macroeconómica; define, formula y ejecuta la política fiscal del país; incide en los sectores económicos, gubernamentales y políticos; y gestiona los recursos públicos de la Nación, desde la perspectiva presupuestal y financiera, mediante actuaciones transparentes, personal competente y procesos eficientes, con el fin de propiciar: Las condiciones para el crecimiento económico sostenible, y la estabilidad y solidez de la economía y del sistema financiero.

EVALUACIÓN DEL RIESGO: Proceso de comparar el riesgo estimado contra criterios de riesgo evidenciados en dados, a fin de determinar la importancia del riesgo.

EVENTO DE SEGURIDAD DE LA INFORMACIÓN: Presencia identificada de una condición de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

FIREWALL (CORTAFUEGOS): Es un dispositivo de seguridad de red que monitorea el tráfico de red entrante y saliente y decide si permitir o bloquear tráfico específico según un conjunto definido de reglas de seguridad.

FUGA DE INFORMACIÓN: Se denomina al incidente (tanto interno como externo, y a la vez intencional o no) que pone en poder de una persona ajena a la organización, información confidencial y que sólo debería estar disponible para integrantes de la misma.

GESTIÓN DEL RIESGO: Actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.

GUSANOS: Son programas maliciosos que se reproducen de un sistema a otro sin usar un archivo anfitrión, lo que contrasta con los virus, puesto que requieren la propagación de un archivo anfitrión infectado.

HARDWARE: Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.

DECRETO N°
(135)

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: Evento o serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

INGENIERÍA SOCIAL: Método utilizado por los atacantes para engañar a los usuarios informáticos, para que realicen una acción que normalmente producirá consecuencias negativas, como la descarga de malware o la divulgación de información personal. Los ataques de phishing con frecuencia aprovechan las tácticas de ingeniería social.

INTEGRIDAD: La Integridad es la propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software o hardware o por condiciones medioambientales.

IMPACTO: Es el resultado obtenido a partir de la materialización de una amenaza.

MALWARE: Es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. El malware a menudo utiliza herramientas de comunicación populares, como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse. También se propaga a través de descargas inadvertidas y ataques a las vulnerabilidades de seguridad en el software. La mayoría del malware peligroso actualmente busca robar información personal que pueda ser utilizada por los atacantes para cometer delitos.

MINTIC: Ministerio de Tecnologías de la Información y Comunicaciones.

MSPI: es la sigla del Modelo de Seguridad y Privacidad de la Información.

POLÍTICA DE SEGURIDAD: Son las decisiones o medidas de seguridad que una empresa ha decidido tomar respecto a la seguridad de sus sistemas de información después de evaluar el valor de sus activos y los riesgos a los que están expuestos.

PROBABILIDAD DE OCURRENCIA: Estimación de ocurrencia de un evento, el cual está relacionado a características de las vulnerabilidades presentadas y el origen de la amenaza.

RIESGO: Posibilidad de que algo suceda que impactará en los objetivos. Se mide en términos de consecuencias y probabilidad.

RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN: Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización

RIESGO RESIDUAL: Nivel restante de riesgo después del tratamiento del riesgo.

DECRETO N°
(-- 135)

ROUTER (ENRUTADOR): Se trata de un producto de hardware que permite interconectar computadoras que funcionan en el marco de una red

SEGURIDAD DE LA INFORMACIÓN: Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad.

SI: Sistema de Información.

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN SGSI: Parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

SOFTWARE: Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.

SPAM: También conocido como correo basura, el spam es correo electrónico que involucra mensajes casi idénticos enviados a numerosos destinatarios. Un sinónimo común de spam es correo electrónico comercial no solicitado (UCE). El malware se utiliza a menudo para propagar mensajes de spam al infectar un equipo, buscar direcciones de correo electrónico y luego utilizar esa máquina para enviar mensajes de spam.

TRATAMIENTO DEL RIESGO: Proceso de selección e implementación de medidas para modificar el riesgo.

VALORACIÓN DEL RIESGO: Proceso global de análisis y evaluación del riesgo.

VIRUS: Programa diseñado para que al momento de ejecutarse, se copie a sí mismo adjuntándose en aplicaciones existentes en el equipo. De esta manera, cuando se ejecuta una aplicación infectada, puede infectar otros archivos. A diferencia de otro tipo de malware, como los gusanos, se necesita acción humana para que un virus se propague entre máquinas y sistemas.

Los efectos que pueden provocar varían dependiendo de cada tipo de virus: mostrar un mensaje, sobrescribir archivos, borrar archivos, enviar información confidencial mediante correos electrónicos a terceros, etc. Los más comunes son los que infectan a ficheros ejecutables.

VULNERABILIDAD: Cualquier debilidad que pueda ser aprovechada por una amenaza.

ZERO-DAY (DÍA CERO): Son aquellas vulnerabilidades en sistemas o programas informáticos que son únicamente conocidas por determinados atacantes y son desconocidas por los fabricantes y usuarios. Al ser desconocidas por los fabricantes, no existe un parche de seguridad para solucionarlas. Por esta razón son muy peligrosas ya que el atacante puede explotarlas sin que el usuario sea consciente de que es vulnerable.

DECRETO N°
(135)

4. MARCO LEGAL Y/O NORMATIVO

CONSTITUCIÓN POLÍTICA DE COLOMBIA 1991; Artículo 15. "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. Disponible en

LEY 23 DE 1982 sobre Derechos de Autor. Congreso de la República.

LEY 527 DE 1999; por medio de la cual 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 y se dictan otras disposiciones.

LEY 1266 DE 2008, por la cual se dictan las disposiciones generales del hábeas 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 y se dictan otras disposiciones.

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 1474 DE 2011 Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

DECRETO 4632 DE 2011 Por medio del cual se reglamenta parcialmente la Ley 1474 de 2011 en lo que se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones.

LEY ESTATUTARIA 1581 DE 2012, Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República.

DECRETO 2609 DE 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.

DECRETO 2573 de 2014 Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones.

DECRETO 1377 DE 2013 Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

MANUAL GOBIERNO EN LÍNEA 3.1 Ver 2014-06-12. Para la Implementación de la Estrategia de Gobierno en Línea, entidades del orden nacional; Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea; Formato Política SGSI - Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea.

DECRETO N°
(- - 135)

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.

DECRETO 2573 DE 2014 Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 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 1494 DE 2015, Por el cual se corrigen yerros en la Ley 1712 de 2014.

DECRETO 1080 DE 2015: Por medio del cual se expide el Decreto Único Reglamentario del Sector Cultura

ACUERDO 003 DE 2015: 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

DECRETO 1081 DE 2015, Libro 2 Parte 1 Título 1: Disposiciones generales en materia de transparencia y del derecho de acceso a la información pública nacional

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 1499 DE 2017: Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015

LEY 1955 DE 2019: por el cual se expide el Plan Nacional de Desarrollo 2018-2022. "Pacto por Colombia, Pacto por la Equidad".

CONPES 3701 LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA

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 número 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

CONPES 3995 Política Nacional de Confianza y Seguridad Digital.

RESOLUCIÓN 500 DE 2021 Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el Modelo de Seguridad y Privacidad como habilitador de la política de Gobierno Digital

5. POLÍTICA

DECRETO N°
(135)

LA ALCALDÍA MUNICIPAL DE SOPÓ, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes colombianas vigentes y en concordancia con la misión y visión de la entidad.

Para **LA ALCALDÍA MUNICIPAL DE SOPÓ**, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes 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 ciudadanos, contratistas y funcionarios.
- Brindar soporte sobre las innovaciones tecnológicas que se implementen.
- Proteger los activos tecnológicos.
- 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 ALCALDÍA MUNICIPAL DE SOPÓ**
- Garantizar la continuidad de los procesos frente a incidentes.
- **LA ALCALDÍA MUNICIPAL DE SOPÓ** 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 de los procesos, y a los requerimientos regulatorios.

A continuación, se establecen los principios de seguridad que soportan el SGSI de **LA ALCALDÍA MUNICIPAL DE SOPÓ**:

• Las **responsabilidades** frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de **los empleados, proveedores, socios o terceros**.

• **LA ALCALDÍA MUNICIPAL DE SOPÓ protegerá la información** generada, procesada o resguardada por los procesos, su infraestructura tecnológica y activos del riesgo que se genera de los accesos **otorgados a terceros** (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.

• **LA ALCALDÍA MUNICIPAL DE SOPÓ protegerá la información** creada, procesada, transmitida o resguardada por sus procesos, con el fin de minimizar impactos financieros, operativos o legales debido a un **uso incorrecto** de ésta.

DECRETO N°
(- 135)

Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

• **LA ALCALDÍA MUNICIPAL DE SOPÓ protegerá su información** de las amenazas originadas por parte **del personal**.

• **LA ALCALDÍA MUNICIPAL DE SOPÓ protegerá las instalaciones** de procesamiento y la infraestructura tecnológica **que soporta sus procesos críticos**.

• **LA ALCALDÍA MUNICIPAL DE SOPÓ controlará la operación** de sus procesos garantizando la seguridad de los recursos tecnológicos y las redes de datos.

• **LA ALCALDÍA MUNICIPAL DE SOPÓ implementará control de acceso** a la información, sistemas y recursos de red.

• **LA ALCALDÍA MUNICIPAL DE SOPÓ** garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

• **LA ALCALDÍA MUNICIPAL DE SOPÓ** 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.

• **LA ALCALDÍA MUNICIPAL DE SOPÓ garantizará la disponibilidad** de sus procesos y la continuidad de su operación basada en el impacto que pueden generar los eventos.

• **LA ALCALDÍA MUNICIPAL DE SOPÓ** garantizará el cumplimiento de las **obligaciones legales, regulatorias y contractuales establecidas.**

5.1. RESPONSABILIDADES FRENTE A LA SEGURIDAD DE LA INFORMACIÓN Y AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

5.1.1. RESPONSABILIDADES DEL ÁREA DE SISTEMAS DE INFORMACIÓN

- Establecer, mantener y divulgar las políticas y procedimientos de servicios de tecnología, incluida esta política de seguridad de información y todos sus capítulos, el uso de los servicios tecnológicos en toda la entidad de acuerdo a las mejores prácticas y lineamientos de la Alta Dirección de la entidad y directrices del Gobierno.
- Mantener la custodia de la información que reposa en los diferentes sistemas de información, bases de datos y aplicativos de la entidad.
- Informar de los eventos que estén en contra de la seguridad de la información y de la infraestructura tecnológica de la entidad a la Secretaría de Desarrollo Institucional.
- Proporcionar medidas de seguridad físicas, lógicas y procedimentales para la protección de la información digital de la entidad.
- Administrar las reglas y atributos de acceso a los equipos de cómputo, sistemas de información, aplicativos y demás fuentes de información al servicio de la entidad.

- Analizar, aplicar y mantener los controles de seguridad implementados para asegurar los datos e información gestionados en la entidad.
- Habilitar/Deshabilitar el reconocimiento y operación de Dispositivos de Almacenamiento externo de acuerdo con las directrices emitidas de parte de la Secretaría de Desarrollo Institucional.
- Garantizar la disponibilidad de los servicios y así mismo programar o informar a todos los usuarios cualquier problema o mantenimiento que pueda afectar la normal prestación de los mismos; así como gestionar su acceso de acuerdo a las solicitudes recibidas de las diferentes secretarías, siguiendo el procedimiento establecido.
- Determinar las estrategias para el mejoramiento continuo del servicio tecnológico, la optimización de los recursos tecnológicos, las mejoras en los sistemas de información con miras a un gobierno de tecnologías consolidado.
- Gestionar ante la Alta Dirección y ante los responsables del presupuesto, los elementos necesarios para brindar un entorno de seguridad de la información en la entidad.
- Generar los espacios y los procesos necesarios para las capacitaciones y sensibilizaciones en seguridad y privacidad de la información.
- Brindar el soporte y mantenimientos necesarios a los usuarios a través de los canales de mesa de ayuda actualmente implementados en la entidad.
- Garantizar que la entrega de los elementos y equipos se realice mediante acta suscrita con el respectivo funcionario responsable.

5.1.2. RESPONSABILIDADES DE LOS PROPIETARIOS DE LA INFORMACIÓN

Son propietarios de la información cada uno de los secretarios, así como los directores y/o jefes de las oficinas donde se genera, procesa y mantiene información, en cualquier medio, propia del desarrollo de sus actividades.

- Valorar y clasificar la información que está bajo su administración y/o generación.
- Autorizar, restringir y delimitar a los demás usuarios de la entidad el acceso a la información de acuerdo a los roles y responsabilidades de los diferentes funcionarios, contratistas o practicantes que por sus actividades requieran acceder a consultar, crear o modificar parte o la totalidad de la información.
- Determinar los tiempos de retención de la información en conjunto con el grupo de Gestión Documental y Correspondencia y las áreas que se encarguen de su protección y almacenamiento de acuerdo a las determinaciones y políticas de la entidad como de los entes externos y las normas o leyes vigentes.
- Determinar y evaluar de forma permanente los riesgos asociados a la información, así como los controles implementados para el acceso y gestión de la administración comunicando cualquier anomalía o mejora tanto a los usuarios como a los custodios de la misma.
- Acoger e informar los lineamientos de esta política a todos los funcionarios, contratistas y practicantes en las diferentes dependencias de la entidad.

DECRETO N°
(- - 135)

5.1.3. RESPONSABILIDADES DE LOS FUNCIONARIOS USUARIOS DE LA INFORMACIÓN

- Utilizar solamente la información necesaria para llevar a cabo las funciones que le fueron asignadas, de acuerdo con los permisos establecidos o aprobados en el Manual de Funciones.
- Manejar la Información de la entidad y rendir cuentas por el uso y protección de tal información, mientras que este bajo su custodia. Esta puede ser física o electrónica e igualmente almacenada en cualquier medio.
- Proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.
- Evitar la divulgación no autorizada o el uso indebido de la información.
- Cumplir con todos los controles establecidos por los propietarios de la información y los custodios de la misma.
- Informar a sus superiores sobre la violación de estas políticas o si conocen de alguna falta a alguna de ellas.
- Proteger los datos almacenados en los equipos de cómputo y sistemas de información a su disposición, de la destrucción o alteración intencional o no justificada y de la divulgación no autorizada.
- Reportar los Incidentes de seguridad, eventos sospechosos y el mal uso de los recursos que identifique.
- Proteger los equipos de cómputo, de comunicaciones y demás dispositivos tecnológicos o técnico-científicos designados para el desarrollo de sus funciones. No está permitida la conexión de equipos de cómputo y de comunicaciones ajenos a la entidad a la red Institucional ni el uso de dispositivos de acceso externo a Internet o de difusión de señales de red que no hayan sido previamente autorizadas por el Área de Sistemas de la entidad.
- Usar software autorizado que haya sido adquirido legalmente por la Institución. No está permitido la instalación ni uso de software diferente al Institucional en ninguna circunstancia.
- Divulgar, aplicar y cumplir con la presente Política.
- Aceptar y reconocer que en cualquier momento y sin previo aviso, la Dirección de la entidad puede solicitar una inspección de la información a su cargo sin importar la ubicación de esta información o medio de almacenamiento. Esto incluye todos los datos y archivos de los correos electrónicos institucionales, sitios web institucionales y redes sociales propiedad de la entidad, al igual que las unidades de red institucionales, computadoras, servidores u otros medios de almacenamiento propios de la entidad. Esta revisión puede ser requerida para asegurar el cumplimiento de las políticas internamente definidas, por actividades de auditoría y control interno o en el caso de requerimientos de entes fiscalizadores y de vigilancia externos, legales o gubernamentales.
- Proteger y resguardar su información personal que no esté relacionada con sus funciones en la Institución (Cuentas de correo electrónico, cuentas bancarias, etc.). **LA ALCALDÍA MUNICIPAL DE SOPÓ no** es responsable por la pérdida de información, desfalco o daño que pueda tener un usuario al brindar información personal como identificación de

usuarios, claves, números de cuentas o números de tarjetas débito/crédito.

- Suscribir un Acuerdo de Confidencialidad como un documento en los que los funcionarios de la Alcaldía Municipal de Sopó o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la entidad, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.
- El funcionario se obliga única y exclusivamente a guardar y hacer uso de la herramienta de trabajo con información de la entidad. Queda totalmente prohibido incluir información de carácter íntima y/o personal, y en el evento de no cumplir con esta obligación se hará acreedor a las sanciones a que haya lugar.

5.1.4 RESPONSABILIDADES DE LOS CONTRATISTAS Y PRACTICANTES USUARIOS DE LA INFORMACIÓN

- Utilizar solamente la información necesaria para llevar a cabo las funciones que le fueron asignadas, de acuerdo con los permisos establecidos o aprobados por el Supervisor del Contrato o de las Prácticas.
- Manejar la Información de la entidad y rendir cuentas por el uso y protección de tal información, mientras que este bajo su custodia. Esta puede ser física o electrónica e igualmente almacenada en cualquier medio.
- Proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.
- Evitar la divulgación no autorizada o el uso indebido de la información.
- Cumplir con todos los controles establecidos por los propietarios de la información y los custodios de la misma.
- Informar al supervisor de contrato sobre la violación de estas políticas o si conocen de alguna falta a alguna de ellas.
- Proteger los datos almacenados en los equipos de cómputo y sistemas de información a su disposición, de la destrucción o alteración intencional o no justificada y de la divulgación no autorizada.
- Reportar los Incidentes de seguridad, eventos sospechosos y el mal uso de los recursos que identifique.
- Proteger los equipos de cómputo, de comunicaciones y demás dispositivos tecnológicos o técnico-científicos designados para el desarrollo de sus funciones. No está permitida la conexión de equipos de cómputo y de comunicaciones ajenos a la entidad a la red Institucional ni el uso de dispositivos de acceso externo a Internet o de difusión de señales de red que no hayan sido previamente autorizadas por el Área de Sistemas de la entidad.
- Divulgar, aplicar y cumplir con la presente Política.
- Proteger y resguardar su información personal que no esté relacionada con sus funciones en la Institución (Cuentas de correo electrónico, cuentas bancarias, etc.). **LA ALCALDÍA MUNICIPAL DE SOPÓ no** es responsable por la pérdida de información, desfalco o daño que pueda tener un usuario al brindar información personal como identificación de

usuarios, claves, números de cuentas o números de tarjetas débito/crédito.

- Acuerdo de Confidencialidad: es un documento en los que los funcionarios de la Alcaldía Municipal de Sopó o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la entidad, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.

6. LINEAMIENTOS POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

6.1. USO DE USUARIOS Y CONTRASEÑAS

Expone las condiciones, normas y procedimientos necesarios para fijar los requisitos que se deben cumplir por cualquier funcionario, contratista o practicante de la entidad para obtener acceso a los sistemas de información, hardware y software propiedad de la ALCALDÍA MUNICIPAL DE SOPÓ.

La asignación de usuarios y contraseñas es un permiso que LA ALCALDÍA MUNICIPAL DE SOPÓ otorga a sus funcionarios, contratistas o practicantes con el fin de que tengan acceso a los recursos tecnológicos como a las plataformas y sistemas de información que permiten la operación, consulta y resguardo de la información institucional.

Los objetivos específicos de los lineamientos para el uso de usuarios y contraseñas son:

- Presentar a todos los funcionarios y contratistas de LA ALCALDÍA MUNICIPAL DE SOPÓ responsables de la asignación, creación y modificación de usuarios y contraseñas las directrices a seguir y verificar que se cumplan a cabalidad con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información de LA ALCALDÍA MUNICIPAL DE SOPÓ.
- Se debe concientizar y controlar a los usuarios para que apliquen buenas prácticas de seguridad en la selección, uso y protección de claves o contraseñas, las cuales constituyen un medio de validación de la identidad de un usuario y consecuentemente un medio para establecer derechos de acceso a las instalaciones, equipos o servicios informáticos.
- Concientizar a todos los funcionarios, contratistas o practicantes sobre los riesgos asociados con el uso de las credenciales de acceso (usuario y contraseña) y las consecuencias de exponer de manera inadecuada la identidad ante cualquier tercero, en el entendido que los usuarios y claves asignados a cada funcionarios, contratistas o practicantes son personales e intransferibles.
- Asegurar el correcto manejo de la información sensible y privada de la entidad.

La asignación de credenciales: usuarios (Login o UserId) y contraseñas (Clave o Password) a los diferentes funcionarios, contratistas o practicantes, así como su desactivación de los sistemas se harán de acuerdo a los procedimientos establecidos y según sea solicitado por los secretarios de dependencias, jefes de oficina o por la dependencia de Desarrollo Institucional.

Las cuentas de usuario son entera responsabilidad del funcionario, contratista o practicante al que se le asigne. La cuenta es para uso personal e intransferible.

Las cuentas de usuario (usuario y clave) son sensibles a mayúsculas y minúsculas, es decir que estas deben ser tecleadas como se definan.

De ser necesaria la divulgación de la cuenta de usuario y su contraseña asociada, debe solicitarlo por escrito y dirigido al Área de Sistemas de Información de la ALCALDÍA MUNICIPAL DE SOPÓ.

Si se detecta o sospecha que las actividades de una cuenta de usuario pueden comprometer la integridad y seguridad de la información, el acceso a dicha cuenta es suspendido temporalmente y es reactivada sólo después de haber tomado las medidas necesarias a consideración del Área de Sistemas de Información.

6.1.2. TIPOS DE CUENTAS DE USUARIO

Todas las cuentas de acceso a las plataformas tecnológicas como a los sistemas de información y aplicaciones son propiedad de la Institución. Para efectos del presente lineamiento, se definen dos tipos de cuentas:

6.1.2.1. Cuenta de Usuario de Sistema de Información:

Son todas aquellas cuentas que sean utilizadas por los usuarios para acceder a los diferentes sistemas de información. Estas cuentas permiten el acceso para consulta, modificación, actualización o eliminación de información, y se encuentran reguladas por los roles de usuario de cada Sistema de Información en particular.

6.1.2.2. Cuenta de Administración de Sistema de Información:

Corresponde a la cuenta de usuario que permite al administrador del Sistema, plataforma tecnológica o base de datos realizar tareas específicas de usuario a nivel administrativo, como, por ejemplo: agregar/modificar/eliminar cuentas de usuario del sistema. Usualmente estas cuentas están asignadas para su gestión por parte del Área de Sistemas de Información, y debe seguir las siguientes indicaciones de manejo:

1. Todas las contraseñas deben ser tratadas con carácter confidencial.
2. Las contraseñas de ninguna manera podrán ser transmitidas mediante servicios de mensajería electrónica instantánea ni vía telefónica.
3. Se evitará mencionar y en la medida de lo posible, teclear las contraseñas en frente de otros.
4. Se evitará el revelar contraseñas en cuestionarios, reportes o formularios.
5. Se evitará el utilizar la misma contraseña para acceso a los sistemas operativos y/o a las bases de datos u otras aplicaciones.
6. Se evitará el activar o hacer uso de la utilidad de recordar clave o recordar Password de las aplicaciones.

6.1.3. Uso apropiado de usuarios y contraseñas:

- Usar las credenciales de acceso sobre los sistemas otorgados exclusivamente para fines laborales y cuando sea necesario en cumplimiento de las funciones asignadas.
- Cambiar periódicamente las contraseñas de los sistemas de información o servicio tecnológicos autorizados.
- Las contraseñas deben poseer algún grado de complejidad y no deben ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, ni productos a resaltar de la ALCALDÍA MUNICIPAL DE SOPÓ, evite asociarla con eventos u ocasiones especiales, por ejemplo: fechas de cumpleaños, nombre de los hijos, placas de automóvil, etc.
- Nunca utilice sus contraseñas personales en el entorno laboral.
- Cambiar la contraseña si ha estado bajo riesgo o se ha detectado anomalía en la cuenta de usuario.
- No se deben usar caracteres idénticos consecutivos, ni que sean todos numéricos, ni todos alfabéticos, sino que se deben combinar letras en mayúscula, minúscula, números y caracteres especiales (Símbolos), con una longitud mínima de ocho (8) caracteres.
- Al momento de realizar una entrega de cargo se debe dejar en acta de entrega las credenciales de los sistemas de información a los cuales se tienen acceso y será responsabilidad del Secretario de esa dependencia o Jefe inmediato supervisar el cambio del usuario si es necesario y su respectiva contraseña.

6.1.4. Uso indebido del servicio de usuarios y contraseñas:

- Permitir el conocimiento de las claves a terceros.
- Almacenar las credenciales de acceso en libretas, agendas, post-it, hojas sueltas, etc.
- Almacenar las credenciales sin protección, en sistemas electrónicos personales (Tablets, memorias USB, teléfonos celulares, agendas electrónicas, etc.).
- Intentar acceder de forma no autorizada con otro usuario y clave diferente a la personal en cualquier sistema de información o plataforma tecnológica.
- Usar identificadores de terceras personas para acceder a información no autorizada o suplantar al usuario respectivo.
- Utilizar su usuario y contraseña para propósitos comerciales ajenos al Institucional.
- Intentar o modificar los sistemas y parámetros de la seguridad de los sistemas de la red de LA ALCALDÍA MUNICIPAL DE SOPÓ.

6.1.5. Responsabilidades de los funcionarios, contratistas y practicantes con usuarios y contraseñas asignados

- Conocer, adoptar y acatar este lineamiento.
- Velar por la seguridad de la información a la que tenga acceso a través de las credenciales asignadas y a los sistemas de información autorizados para su acceso.
- Al retirarse de su equipo en cualquier momento, bloquear su sesión de trabajo para evitar el uso de su identidad y/o acceso a documentos no autorizados.

- Dar aviso al Área de Sistemas, a través de los medios establecidos, de cualquier fallo de seguridad, incluyendo su uso no autorizado, pérdida de la contraseña, suplantación, etc.

6.1.6. Monitoreo:

- El administrador de los sistemas de información, bases de datos y plataformas tecnológicas puede efectuar una revisión periódica de los accesos exitosos y no exitosos y al número de intentos efectuados a dichos sistemas para determinar posibles accesos indebidos o no autorizados.

- El Área de Sistemas podrá revisar las bitácoras y registros de control de los usuarios que puedan afectar la operación de cualquier sistema o plataforma.

- El Área de Sistemas podrá restringir el acceso a cualquier cuenta y sin previo aviso si se evidencia un mal manejo o riesgo desde la misma.

6.2. USO DEL SERVICIO DE CORREO ELECTRÓNICO DE LA ALCALDÍA MUNICIPAL DE SOPÓ

Concienciar a los funcionarios, contratistas o practicantes de la ALCALDÍA MUNICIPAL DE SOPÓ de los riesgos asociados con el uso de correo electrónico y presenta las normas y protocolos a seguir para el buen uso de este servicio.

El correo electrónico es un servicio basado en el intercambio de información a través de la red y el cual es provisto por LA ALCALDÍA MUNICIPAL DE SOPÓ para los funcionarios y contratistas previamente autorizados para su acceso.

Los objetivos específicos de los lineamientos para el uso del correo electrónico son:

- Incentivar el uso del servicio de correo electrónico para fines estrictamente laborales de LA ALCALDÍA MUNICIPAL DE SOPÓ.
- Asegurar el correcto manejo de la información privada de la entidad por parte de los funcionarios, contratistas o practicantes de la entidad.
- Garantizar la confidencialidad, la privacidad y el uso adecuado y moderado de la información a través de este servicio.

El acceso al correo electrónico es un servicio otorgado por LA ALCALDÍA MUNICIPAL DE SOPÓ a sus funcionarios y contratistas y el mismo sobrelleva responsabilidades y compromisos para su uso.

LA ALCALDÍA MUNICIPAL DE SOPÓ a criterio propio puede otorgar el acceso a los servicios de correo electrónico para la realización de actividades institucionales al personal de planta y contratistas. El acceso incluye la preparación, transmisión, recepción y almacenamiento de mensajes de correo electrónico y sus adjuntos. Los secretarios, jefes o coordinadores tienen la autonomía de otorgar y solicitar el acceso de sus funcionarios, contratistas o practicantes a este servicio.

DECRETO N°
(135)

Las credenciales de los usuarios serán desactivadas de los sistemas de acuerdo a los procedimientos establecidos y según sea solicitado por los secretarios, jefes de oficina o por el equipo de Desarrollo Institucional.

La falla consecutiva, después múltiples intentos de acceso a la cuenta vía web ocasiona el bloqueo de la cuenta y esta se desbloquea por solicitud al Área de Sistemas de Información.

Cuentas temporales:

Estas cuentas son creadas en forma temporal, con una vigencia definida previamente, con propósitos específicos de comunicación derivados de contratos temporales o provisionales. Estas cuentas tendrán una fecha de caducidad y se desactivarán automáticamente a su término, a menos que se solicite lo contrario. Se abrirán con una vigencia no mayor de 3 meses y podrán renovarse por periodos máximos similares.

Todo correo electrónico que sea enviado fuera de la ALCALDÍA MUNICIPAL DE SOPÓ, a través de este servicio de correo, contendrá la siguiente clausula al pie de página del mensaje del mismo:

"Este correo electrónico y cualquier archivo(s) adjunto al mismo, contiene información de carácter confidencial exclusivamente dirigida a su destinatario(s). Si usted no es el destinatario indicado, queda notificado que la lectura, utilización, divulgación y/o copia sin autorización está prohibida en virtud de la legislación vigente. En el caso de haber recibido este correo electrónico por error, agradecemos informarnos inmediatamente de esta situación mediante el reenvío a la dirección electrónica del remitente. Las opiniones que contenga este mensaje son exclusivas de su autor y no necesariamente representan la opinión oficial de la ALCALDÍA MUNICIPAL DE SOPÓ."

This email and any file(s) attached to it contain confidential information that is exclusively addressed to its recipient(s). If you are not the indicated recipient, you are informed that reading, using, disseminating and/or copying it without authorization is forbidden in accordance with the legislation in effect. If you have received this email by mistake, please immediately notify the sender of the situation by resending it to their email address. The opinions contained in this message are solely those of the author and do not necessarily represent the official views of "ALCALDÍA MUNICIPAL DE SOPÓ."

6.2.1. Uso apropiado de los servicios de correo electrónico de la ALCALDÍA MUNICIPAL DE SOPÓ

- Conservar normas de respeto, confidencialidad y criterio ético por parte de todos los funcionarios y contratistas con acceso a este servicio.
- Usar el correo electrónico Institucional exclusivamente para fines laborales: para la difusión o el envío de circulares, memorandos, oficios y archivos de trabajo, cuando sea necesario en cumplimiento de las funciones asignadas.
- Redactar los contenidos de un mensaje de correo electrónico de tal manera que sea serio, claro, conciso, cortés y respetuoso de acuerdo al

protocolo de atención al ciudadano ya establecido por la Alcaldía Municipal de Sopó.

- Ingresar a las cuentas de correo de cada usuario a través de los medios que la entidad destina, que en este caso se realizará vía Gmail a través del navegador. Cada funcionario o contratista autorizado tendrá una credencial de acceso conformada por un usuario y una clave asignada por el encargado de su administración, para el caso de la ALCALDÍA MUNICIPAL DE SOPÓ es el Área de Sistemas de Información a través de los procedimientos establecidos, una vez entregada esta clave el usuario debe cambiarla para poder acceder al buzón.

6.2.2. Uso indebido del servicio de correo electrónico de LA ALCALDÍA MUNICIPAL DE SOPÓ

- Participar en la difusión de "cartas en cadenas", en esquemas piramidales o de propagandas dentro y fuera de la institución.
- Realizar intentos no autorizados para acceder a otra cuenta de correo electrónico Institucional.
- Revelar o publicar cualquier información clasificada o reservada de la ALCALDÍA MUNICIPAL DE SOPÓ.
- Descargar, enviar, imprimir o copiar documentos o contenidos en contra de las leyes de derechos de autor.
- Copiar ilegalmente o reenviar mensajes que hayan sido restringidos por parte del usuario o el emisor.
- Descargar cualquier software o archivo sin tomar las medidas de precaución para evitar el acceso de virus en las redes y equipos informáticos.
- Utilizar expresiones difamatorias o groseras en contra de individuos, clientes o entidades públicas o privadas. Los mensajes enviados a través de este servicio no pueden contener material insidioso, ofensivo, obsceno, vulgar, racista, pornográfico, subversivo u otro material no formal.
- Enviar información clasificada o reservada de la ALCALDÍA MUNICIPAL DE SOPÓ por medio de canales no seguros (no codificados) como es Internet y/o las cuentas de correo de uso público (Gmail Personal, Hotmail, Yahoo!, etc.).
- Participar en actividades que puedan causar congestión o interrupción en los servicios de comunicación de la ALCALDÍA MUNICIPAL DE SOPÓ o la normal operación de los servicios de correo electrónico.
- Enviar correos SPAM de cualquier índole.
- Reenviar correos con contenido PHISHING.
- Usar seudónimos y enviar mensajes anónimos, así como aquellos que consignen títulos, cargos o funciones no oficiales.
- Utilizar el correo electrónico para propósitos comerciales ajenos al Institucional.
- Eliminar o modificar la firma del correo institucional a la hora de realizar el envío de un mensaje sin las autorizaciones correspondientes.
- Intentar o modificar los sistemas y parámetros de la seguridad de los sistemas de la red de la ALCALDÍA MUNICIPAL DE SOPÓ
- Utilizar mecanismos y sistemas que intenten ocultar o suplantar la identidad del emisor de correo.
- Usar correos públicos para la recepción, envío o distribución de información pública clasificada o reservada propia de la ALCALDÍA MUNICIPAL DE SOPÓ.

DECRETO N°
(135)

- Configurar y conectar los clientes de correo electrónico con los sitios de redes sociales que no sean autorizadas por la entidad o que no pertenezcan a ninguna red de carácter oficial.
- Distribuir listas de direcciones de correo personales sin expresa autorización de sus dueños.
- Enviar archivos con extensión .exe, .pif, .scr, .vbs, .cmd, .com, .bat, .hta, .dll debido a que este tipo de extensiones son propensas a ser utilizadas para propagación de virus.
- Enviar contenidos multimedia (video o audio) con extensión .wav, .mp3, .mp4, .mpeg, .wma, .wmv, .mov, .asf, .flv ya que estos documentos son muy pesados y ralentizan la red de comunicaciones, a su vez llenan el buzón de correo.

El uso inapropiado o el abuso en el servicio de correo electrónico ocasionan la desactivación temporal o permanente de las cuentas. La desactivación de la cuenta lleva consigo la imposibilidad de acceder a los mensajes de correo que estén en ese momento en el servidor y la imposibilidad de recibir nuevos mientras no vuelva a ser activada.

6.2.3. Envío y transferencia sobre el servicio de correo electrónico

- La capacidad del buzón del servidor de correo de cada funcionario o contratista es de 30 GB incluyendo la papelera de reciclaje, los mensajes enviados y el sistema de nube del buzón (Drive). En determinadas ocasiones será necesario que los usuarios liberen espacio en el buzón de correo, eliminando los correos que ya no sean necesarios, descargando los anexos a su computadora institucional.
- Una vez superada la cuota asignada por usuario los mensajes no pueden ser descargados a sus buzones locales hasta no liberar el espacio necesario del servidor de correo, esta liberación la debe hacer cada usuario depurando los correos innecesarios, borrando las bandejas de spam y eliminados.
- El tamaño máximo de cada mensaje de correo electrónico no debe exceder los 20 MB a las limitaciones propias de los buzones. Esto tiene efecto tanto para el envío como para la recepción.
- Se recomienda el uso del campo CCO: para mantener la privacidad de los correos electrónicos de los destinatarios. Este campo hace que los destinatarios reciban el mensaje sin aparecer en ninguna lista ni ser visibles a los demás, también se debe usar cuando se va a enviar mensajes de citaciones, invitaciones a eventos, etc, para evitar ser reportados en listas de spam.
- Es una buena práctica comprimir los archivos a enviar a través de este servicio, para disminuir las exigencias técnicas en su transmisión.
- Los mensajes destinados a dominios (cuentas) no válidas se rechazan inmediatamente para evitar que direcciones erróneas (por ejemplo, mal escrito) sean aceptadas por el servidor como válidas.
- Se aplican políticas de filtrado de mensajes para evitar en la medida de lo posible la llegada de correo no deseado (SPAM) a los buzones de los usuarios.
- Un mensaje no se acepta cuando provenga de un servidor identificado como fuente de SPAM o como un servidor no válido para el envío de correo electrónico por alguna de las listas de bloqueo.

DECRETO N°
(135)

6.2.4. Responsabilidades de los funcionarios y contratistas que sean usuarios de los servicios de correo electrónico de la ALCALDÍA MUNICIPAL DE SOPÓ

- Cuidar y revisar el contenido de los correos electrónicos que se envíen a través de su cuenta. El uso no autorizado de una cuenta de correo electrónico es ilegal de conformidad con la Ley 1273 de 2009 y constituye una violación de la Política del SGSI de la **ALCALDÍA MUNICIPAL DE SOPÓ.**
- Usar correctamente las credenciales de ingreso (usuario y clave) asignadas.
- La cuenta de correo que proporciona la entidad es personal e intransferible, por lo que no debe compartirse con otras personas.
- Cerrar totalmente la sesión de lectura y envío de correos para evitar el uso de su identidad, cuando se retire del equipo en que se encuentre configurada la cuenta de correo.
- Dar aviso a la Área de Sistemas de Información a través de los medios establecidos, de cualquier fallo de seguridad en su cuenta de correo, incluyendo su uso no autorizado, pérdida de la contraseña, suplantación, etc.
- Responsabilizarse por la información o contenido que sea transmitido a través de la cuenta de correo asignada. Los usuarios del servicio deben considerar que los mensajes enviados a un destinatario pueden ser reenviados a cualquier número de cuentas de correo de otros individuos o grupos.
- Todo usuario es responsable por la destrucción de los mensajes cuyo origen sea desconocido y por lo tanto asumirá la responsabilidad y las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. En estos casos no se debe contestar dichos mensajes, ni abrir los archivos adjuntos y se debe reenviar el correo a la cuenta sistemas1@sopo-cundinamarca.gov.co con la frase "correo sospechoso" en el asunto.

El único servicio de correo electrónico autorizado en la entidad es el asignado por el Área de Sistemas de Información.

6.2.5. Monitoreo

- La entidad tiene el derecho a acceder y revelar los contenidos de los correos electrónicos institucionales de sus funcionarios y contratistas y estos deben dar su consentimiento a la Alcaldía Municipal de Sopó en caso de que algún ente fiscalizador a nivel interno o externo requiera esta información. Priman las exigencias de carácter legal o disciplinario.
- El personal del área de sistemas puede monitorear el cumplimiento de las directrices institucionales en el momento que así lo considere o le sea requerido, con las autorizaciones pertinentes para asegurar la integridad y confidencialidad del sistema.

6.3. USO DEL SERVICIO DE INTERNET/INTRANET DE LA ALCALDÍA MUNICIPAL DE SOPÓ

DECRETO N°
(-735)

Concienciar a los funcionarios, contratistas o practicantes de la entidad de las buenas prácticas a seguir sobre las normas de uso del servicio de Internet/Intranet, así como el conocimiento de los riesgos asociados por el uso indebido de los mismos.

6.3.1. Los objetivos específicos del uso de servicio de internet/intranet

- Incentivar el uso del servicio de Internet/Intranet para fines estrictamente laborales de la Alcaldía Municipal de Sopó.
- Asegurar el correcto manejo de la información privada de la Institución.
- Garantizar la confidencialidad, la privacidad y de uso adecuado y moderado de la información a través de este servicio.

El servicio de Internet/Intranet es un servicio de gran importancia en el mundo laboral, de conocimiento y negocios basado en el acceso a diferentes fuentes de información en distintas ubicaciones a través de sistemas de cómputo interconectados en red a nivel local y mundial.

El acceso a Internet/Intranet es un servicio otorgado por la Alcaldía Municipal de Sopó a sus funcionarios, contratistas o practicantes y así mismo conlleva responsabilidades y compromisos para su uso. Se espera que los usuarios de este servicio conserven normas de buen uso, confidencialidad y criterio ético.

Cada Secretario, Jefe o Director de área tiene la autonomía de otorgar y solicitar el acceso de sus funcionarios, contratistas o practicantes a este servicio, de acuerdo al procedimiento vigente.

El ingreso a este servicio se realiza por medio de la plataforma que la entidad destina, que para este caso es el navegador de internet instalado en cada máquina.

6.3.2. Uso apropiado del servicio de Internet/Intranet

Todos los funcionarios, contratistas y practicantes con autorización al uso y acceso a estos servicios deben:

- Utilizar este servicio exclusivamente para fines laborales.
- Conservar normas de respeto, confidencialidad y criterio ético por parte de todos los funcionarios, contratistas o practicantes con acceso a este servicio.
- Descargar documentos o archivos tomando las medidas de precaución para evitar el acceso de virus en las redes y equipos informáticos.

6.3.3. Uso indebido del servicio de Internet/Intranet

- Acceder a sitios de juegos o apuestas en línea.
- Acceder a sitios de divulgación, descarga o distribución de películas, videos, música, real audio, webcams, emisoras online, etc. sin previa autorización por parte del Área de Sistemas de Información.
- Acceder y/o descargar material pornográfico u ofensivo.

- Utilizar software o servicios de mensajería instantánea (chat) y redes sociales no instalados o no autorizados por el Área de Sistemas de Información.
- Emplear este servicio para la recepción, envío o distribución de información pública clasificada o reservada de la Alcaldía Municipal de Sopó a través de servicios y cuentas de correo públicos.
- Cargar, descargar, enviar, imprimir o copiar archivos, software o contenidos en contra de las leyes de derecho de autor.
- Utilizar el servicio de Internet/Intranet para propósitos comerciales ajenos a la entidad.
- Intentar o modificar las opciones de configuración y/o parámetros de seguridad de los navegadores instalados por la entidad.
- Interferir intencionalmente con la operación normal de cualquier website o portal en Internet.
- Comprar o vender artículos personales a través de sitios web o de subastas en línea.
- Publicar o enviar opiniones personales, declaraciones políticas y asuntos no propios de la entidad, dirigidos a funcionarios, contratistas o practicantes y público en general, del sector oficial, de otras compañías y organizaciones, a través de este servicio.
- Descargar, instalar y configurar navegadores distintos a los permitidos por el Área de Sistemas de Información.

6.3.4. Responsabilidades de los Usuarios de Internet/Intranet de la ALCALDÍA MUNICIPAL DE SOPÓ

- Conocer, adoptar y acatar esta política cada vez que haga uso de este servicio.
- Dar aviso al Área de Sistemas de Información a través de los medios establecidos de cualquier fallo de seguridad detectado.
- Proteger los derechos de autor de la información obtenida a través de este servicio. Se recomienda citar la fuente (página web) en los documentos o informes generados con información obtenida por este medio.

6.3.5. Monitoreo

- Los funcionarios, contratistas y practicantes deben estar al tanto de que de requerirse información sobre las visitas a los diferentes sitios web ésta se podrá obtener de los equipos sin previo aviso y con autorización del jefe inmediato o Secretario de Despacho encargado, por parte del Área de Sistemas de Información.
- Si se determina que alguna de las páginas previamente restringidas por el Área de Sistemas de Información es requerida para el desempeño de funciones de algún funcionario, contratista o practicante esta será habilitada únicamente con el consentimiento y solicitud de su jefe directo y con el visto bueno del Área de Sistemas de Información.
- Los usuarios del servicio deben considerar que algunos sitios web no son seguros, especialmente los que hacen suplantación de entidades a los bancos y/o emisores de tarjetas de crédito (PHISING) por lo que se recomienda confirmar esta información directamente con las mismas entidades. Igualmente, no se debe proveer información personal ni laboral a sitios de dudosa validez. La Alcaldía Municipal de Sopó no es responsable

por la pérdida de información, desfalco o daño que pueda tener un usuario al acceder a sitios de suplantación o al brindar información personal como identificación de usuarios, claves, números de cuentas o números de tarjetas débito/crédito al hacer el uso de este servicio.

6.4. USO DE DISPOSITIVOS DE ALMACENAMIENTO EXTERNO

Describe el uso permitido de los dispositivos de almacenamiento externo en LA ALCALDÍA MUNICIPAL DE SOPÓ y las restricciones en su empleo al interior de la entidad.

El uso de medios de almacenamiento externo a los disponibles en los diferentes equipos de cómputo, unidades de red compartidas y servidores de la entidad, constituyen una herramienta que sirve para la transferencia rápida y directa de información entre los funcionarios, contratistas o practicantes de la Alcaldía Municipal de Sopó que a la vez puede exponer información confidencial y sensible de la entidad a diversos riesgos y peligros.

6.4.1. Objetivos específicos del uso de dispositivos de almacenamiento externo

- Concientizar a los funcionarios, contratistas o practicantes de la entidad sobre los riesgos asociados con el uso de los medios de almacenamiento, tanto para los sistemas de información como para la infraestructura tecnológica de la Entidad.
- Asegurar el correcto manejo de la información digital que reposa en la entidad.
- Delimitar el uso de estos medios de almacenamiento en las diferentes áreas de la entidad.

La Alcaldía Municipal de Sopó, es consciente que este tipo de herramientas son muy útiles para el resguardo y transporte de información pero igualmente son elementos que permiten extraer información sin dejar huella física ni registro de dicha acción; Por esta razón, la Alcaldía Municipal de Sopó define los compromisos frente al uso de Dispositivos de Almacenamiento Externo para asegurarse de que la información propietaria, adquirida o puesta en custodia en la entidad no está supeditada a fuga, uso no autorizado, modificación, divulgación o pérdida y que esta debe ser protegida adecuadamente según su valor, confidencialidad e importancia.

El uso de dispositivos de almacenamiento externo está permitido en la Alcaldía Municipal de Sopó para los funcionarios, contratistas y practicantes; con el fin de facilitar el compartir y transportar información que no sea de carácter clasificado ni reservado de la entidad dentro de las normas y responsabilidades del manejo de información institucional. Pero se advierte que antes de realizar conexiones al interior de la entidad se deben revisar dichos dispositivos asegurando que se encuentran libres de infecciones.

Los dispositivos de almacenamiento de uso externo comprenden las unidades que se pueden conectar como una memoria USB, por medio de un cable de datos, mediante una conexión inalámbrica directa a cualquier equipo de cómputo de la entidad. Entre estos, se pueden encontrar:

- Memorias Flash USB
- Reproductores portátiles MP3/MP4
- Cámaras con conexión USB
- iPhones/Smartphones
- SD Cards/ Mini SD Cards/ Micro SD Cards.
- PDAS / Tablets
- Dispositivos con tecnología Bluetooth.
- Tarjetas Compact Flash
- Discos duros de uso externo

6.4.2. Uso indebido de dispositivos de almacenamiento externo

- Almacenar o transportar información clasificada o reservada de La Alcaldía Municipal de Sopó.
- Ejecutar programas no autorizados por la ALCALDÍA MUNICIPAL DE SOPÓ desde cualquiera de las unidades de almacenamiento en mención.
- Descargar cualquier archivo sin tomar las medidas de precaución para evitar el acceso de virus en las redes y equipos informáticos.
- Utilizar mecanismos y sistemas que intenten ocultar o suplantar la identidad del usuario de alguno de estos medios de almacenamiento.
- Emplear dispositivos de almacenamiento externo con el fin de almacenar o exponer información sensible o reservada de los usuarios o funcionarios, contratistas o practicantes de la Alcaldía Municipal de Sopó.

En concordancia con lo anterior, y en desarrollo del artículo 19 de la Ley 1712 de 2014, queda RESTRINGIDO el uso de Dispositivos de Almacenamiento Externo, en las siguientes dependencias:

- Secretaría de Hacienda.
- Secretaría de Gobierno (Inspección de Policía, Comisaria de Familia).
- Archivo Central.
- Oficina Asesora Jurídica y Contratación (Área Jurídica)

El área de Sistemas de Información de la Secretaría de Desarrollo Institucional puede en todo momento y en cualquier área o dependencia de la entidad operar, almacenar, adquirir o retirar dispositivos de almacenamiento externo que les permita garantizar la seguridad de la información de la Alcaldía Municipal de Sopó.

6.4.3. Responsabilidades de los usuarios de dispositivos de almacenamiento externo

- Usar de manera responsable la información a su cargo y de los dispositivos de almacenamiento externo que emplee para el transporte de dicha información.
- Velar porque los medios de almacenamiento externo estén libres de software malicioso, espía o virus para lo cual deberá realizar una verificación de dichos dispositivos cada vez que sea conectado a un equipo de cómputo de la entidad por medio del software de protección dispuesto para tal fin.

- En las Secretarías o Áreas con restricción de dispositivos USB se podrán habilitar los puertos, previa solicitud del Secretario de Despacho, el cual será el responsable sobre el uso y manejo de estos dispositivos.

Sera responsabilidad de cada usuario el permitir la utilización de dispositivos de almacenamiento externo en los equipos asignados a él.

6.4.5. Monitoreo

- Los equipos restringidos para el uso de Dispositivos de Almacenamiento Externo se podrán verificar en cualquier momento para corroborar que cuente con los respectivos bloqueos.
- Las entradas de software malintencionado, de espionaje o virus podrán ser detectadas inmediatamente e informadas al Área de Sistemas de Información de la Alcaldía Municipal de Sopó.

6.5. USO DE DISPOSITIVOS DE CAPTURA DE IMÁGENES Y/O GRABACIÓN DE VIDEO y AUDIO

Define el acceso y el uso de cámaras fotográficas, cámaras de video y demás dispositivos que permitan el registro de imágenes, fotografías y/o video en LA ALCALDÍA MUNICIPAL DE SOPÓ.

6.5.1. Objetivos específicos del uso de dispositivos de captura de imágenes y/o grabación de video y audio

- Concientizar a los funcionarios, contratistas, practicantes y demás personas vinculadas con la Alcaldía Municipal de Sopó sobre los riesgos asociados al uso de dispositivos de registros de imagen y/o video, en las instalaciones de la entidad.
- Fortalecer las medidas de seguridad en las áreas de la Alcaldía Municipal de Sopó que gestionan documentos e información de la entidad.
- Dar cumplimiento a las directrices determinadas en la Política de Seguridad de la Información de la entidad.
- Restringir el uso de este tipo de dispositivos en áreas de manejo de información y documentación clasificada o reservada.
- Entre los dispositivos de captura de imágenes y/o grabación de video se pueden encontrar, pero no se limitan a:

  - Cámaras Fotográficas
  - Videocámaras
  - Celulares.
  - iPhones/Smarthphones
  - PDAS/Tablets.
  - WebCams
  - Scanners
  - Impresoras
  - Multifuncionales

La captura de imágenes y/o grabación de video por parte de los ciudadanos o visitantes de la Entidad está prohibida salvo las excepciones permitidas por ley.

No se permite la captura de imágenes y/o grabación de audio/video en las instalaciones o sedes de La Alcaldía Municipal de Sopó (Sede Principal, Casa Bolívar, Oficina de Salud, entre otras), así como del personal por parte de la ciudadanía, funcionarios, contratistas y practicantes de la entidad, sin previa autorización de la Secretaría de Desarrollo Institucional.

El acceso y uso de equipos fotográficos y de video para fines Institucionales, prensa o de comunicación de La Alcaldía Municipal de Sopó debe ser ejercido y/o autorizado previamente por funcionarios de la Oficina Asesora de Comunicaciones.

6.5.2. Responsabilidades de los funcionarios, contratistas y practicantes usuarios de dispositivos de captura de imágenes y/o grabación de video

- Adoptar, poner en práctica, socializar, y acatar estos lineamientos.
- Usar los dispositivos de captura de imágenes y/o grabación de videos que sean de su propiedad o le hayan sido asignadas para el desempeño de sus actividades de acuerdo a lo estipulado anteriormente.
- Abstenerse de fotografiar, escanear, grabar o copiar digitalmente información sensible, clasificada o reservada de la entidad.
- Cumplir con todos los controles establecidos por los propietarios de la información y los custodios de la misma.
- Informar a sus superiores sobre la violación de estos lineamientos o si conocen de alguna falta a alguna de ellas.

6.5.3. Monitoreo

- La Alcaldía Municipal de Sopó puede controlar el acceso de dispositivos de captura de imágenes y/o grabación de video a sus instalaciones en las entradas a cada una de sus secretarías Internas y externas, por medio del personal de vigilancia y seguridad dispuesto en cada uno de los puntos de ingreso de la entidad.
- El monitoreo permanente de uso y manipulación de dispositivos de captura de imágenes y/o grabación de video, es efectuado a través de los sistemas de video vigilancia instalados en las diferentes áreas y sedes de la entidad.

6.6. USO DE ESCRITORIOS Y PANTALLAS DESPEJADAS

Define los mecanismos necesarios que se deben aplicar en la entidad con el fin de proteger la información física residente en los escritorios y puestos de trabajo y la información digital almacenada en los computadores e infraestructura técnica a disposición de todos los funcionarios, contratistas o practicantes para el normal desarrollo de las actividades.

La política de escritorios y pantallas despejadas es extensiva para todos los funcionarios, contratistas y practicantes de la Alcaldía Municipal de Sopó y apoya en la seguridad de la información sensible o crítica de la entidad.

DECRETO N°
(135)

6.6.1. Objetivos específicos para el uso de escritorios y pantallas despejadas

- Garantizar la confidencialidad, la privacidad y el uso adecuado y moderado de la información.
- Crear conciencia sobre los riegos asociados al manejo de información tanto física como digital y la manera de reducirlos aplicando los lineamientos aquí determinados.
- Especificar las recomendaciones y pautas necesarias para mantener las pantallas y escritorios organizados y controlando el reposo de información clasificada o reservada a la vista.
- Dictar las pautas para mantener organizados y resguardados los documentos digitales y correos electrónicos en los computadores puestos a disposición de todos los usuarios de los sistemas de información y estructura tecnológica de la Alcaldía Municipal de Sopó.

Este lineamiento se define en el uso adecuado y ordenado de las áreas de trabajo desde el punto de vista físico como tecnológico entendiéndose para tal fin como escritorio el espacio físico o puesto de trabajo asignado a cada funcionario, contratista o practicante de la entidad y pantalla, el área de trabajo virtual sobre el sistema operativo de su computador, que contiene tanto sus carpetas electrónicas como los archivos y accesos a los diferentes aplicativos Institucionales.

El uso y conservación de los puestos de trabajo (escritorios) y de los fondos de escritorio de sus computadores (pantallas) es una responsabilidad de cada uno de los funcionarios, contratistas y practicantes que tengan acceso a la información de la entidad, sea de manera temporal o indefinida, en el normal desarrollo de sus actividades. Para su definición y aplicación se define de la siguiente manera:

6.6.2. Escritorios (Recomendaciones):

- Se deben dejar organizados los puestos y áreas de trabajo, entendiéndose por esto el resguardo de documentos con información clasificada o reservada evitando que queden a la vista o al alcance de la mano de personal ajeno a la misma.
- En la medida de lo posible los documentos con información clasificada o reservada debe quedar bajo llave o custodia en horas no laborables.
- Se debe evitar el retiro de documentos clasificados o reservados de la entidad y en el caso de ser necesario se debe propender por su protección fuera de la Entidad y su pronta devolución al mismo.
- Se deben controlar la recepción, flujo envío de documentos físicos en la Alcaldía Municipal de Sopó por medio de registro de sus destinatarios desde el punto de correspondencia.
- Se debe restringir el fotocopiado de documentos fuera del horario normal de trabajo y fuera de las instalaciones de la Alcaldía Municipal de Sopó. De ser necesario se debe autorizar el retiro de dichos documentos y garantizar su protección y confidencialidad.
- Al imprimir o fotocopiar documentos con información clasificada o reservada, esta debe ser retirada inmediatamente de las impresoras o multifuncionales utilizadas para tal fin. Y no debe ser dejada desatendida sobre los escritorios.

- No se debe reutilizar papel que contenga información clasificada o reservada.

6.6.3. Pantallas (Recomendaciones):

- Los computadores o estaciones de trabajo deben ser bloqueados por los usuarios al retirarse de los mismos y deben ser desbloqueados por medio del usuario y contraseña asignado para su acceso. Es responsabilidad del usuario, asegurar que el equipo tenga la protección adecuada.
- Las áreas de trabajo virtuales "pantallas" del computador deben tener el mínimo de iconos visibles, limitándose estos a los accesos necesarios para la ejecución de la ofimática, accesos a sistemas de información y a carpetas y unidades de red necesarios para la ejecución de las actividades.
- Los documentos digitales deben ser organizados en carpetas y evitar dejarlos a la vista en las pantallas de los computadores.
- Los funcionarios, contratistas y practicantes al retirarse de la entidad deben apagar los computadores asignados. Queda fuera de esta indicación los servidores y estaciones de trabajo utilizados para acceso remoto. Las sesiones activas se deben terminar cuando el usuario finalice las actividades programadas.
- El área de Sistemas de Información determina una configuración automática en todos los equipos de cómputo, propiedad o contratados por la entidad, para que se active el protector de pantalla del computador, bloqueando el acceso al computador al presentarse una inactividad de 15 minutos. Estos pueden ser nuevamente utilizados por los usuarios al volver a realizar la autenticación por medio de los usuarios y contraseñas asignados.
- El fondo de pantalla de cada computador es único para todas las estaciones de trabajo y para todos los usuarios, puede ser cambiado únicamente por el área de Sistemas de Información o de la Secretaría de Desarrollo Institucional.

6.6.4. Monitoreo:

El área de Sistemas de Información de la Alcaldía Municipal de Sopó en conjunto con la Secretaría de desarrollo institucional, sin previo aviso, realizan brigadas de monitoreo para verificar el estado de los computadores, monitores y escritorios virtuales y generar el respectivo informe de lo encontrado.

6.7. USO DE DISPOSITIVOS MÓVILES (TABLETS, CELULARES INSTITUCIONALES)

Define los mecanismos necesarios que se deben aplicar en la entidad con el fin de proteger la información física residente en las tabletas y celulares institucionales asignados a los funcionarios de LA ALCALDÍA MUNICIPAL DE SOPÓ para el normal desarrollo de las actividades.

La política de uso de dispositivos móviles (tablets, celulares institucionales) aplica a todos los funcionarios, contratistas y practicantes de la Alcaldía Municipal de Sopó y apoya en la seguridad de la información sensible o crítica de la entidad.

6.7.1. Objetivos específicos para el uso de dispositivos móviles

- Garantizar la confidencialidad, la privacidad y el uso adecuado y moderado de la información.
- Crear conciencia sobre los riegos asociados al manejo de información a través de las Tablets y celulares institucionales y la manera de reducirlos aplicando los lineamientos aquí determinados.
- Especificar las recomendaciones y pautas necesarias para mantener tanto los dispositivos como la información protegida.
- Dictar las pautas para mantener la operación, y transmisión de la información registrada en las Tablets y celulares institucionales.

6.7.2. Responsabilidades de la Oficina de Tecnologías de la Información y el Grupo de Soporte Tecnológico

- Determinar y avalar las opciones de protección de los dispositivos móviles institucionales que hagan uso de los servicios provistos por la entidad.
- Establecer las configuraciones aceptables para los dispositivos móviles institucionales que hagan uso de los servicios provistos por la Alcaldía Municipal de Sopó.
- Determinar los métodos de protección de acceso (por ejemplo, contraseñas o patrones) para los dispositivos móviles institucionales que serán entregados a los usuarios. Se debe configurar estos dispositivos para que pasado un tiempo de inactividad pasen automáticamente a modo de suspensión y, en consecuencia, se active el bloqueo de la pantalla el cual requerirá el método de desbloqueo configurado.
- Configurar la opción de borrado remoto de información en los dispositivos móviles institucionales, con el fin de eliminar los datos de dichos dispositivos y restaurarlos a los valores de fábrica, de forma remota, evitando así divulgación no autorizada de información en caso de pérdida o hurto.
- Instalar un software de antivirus en los dispositivos móviles institucionales que hagan uso de los servicios provistos por la entidad.

6.7.3. Responsabilidades de los usuarios

- Los usuarios deben evitar usar los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.
- No deben modificar las configuraciones de seguridad de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.
- Aceptar y aplicar la nueva versión de las actualizaciones que sean notificadas en los dispositivos móviles asignados para su uso.
- Evitar hacer uso de redes inalámbricas de uso público, así como deben desactivar las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados.
- Evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público, de hoteles o cafés internet, entre otros.
- Abstenerse de almacenar videos, fotografías o información personal en los dispositivos móviles institucionales asignados

6.7.4. Monitoreo

- El área de Sistemas de Información en conjunto con la Secretaría de desarrollo institucional, sin previo aviso, realizan brigadas de monitoreo para verificar el estado de la Tablets y celulares y generar el respectivo informe de lo encontrado.

6.8. CONEXIONES REMOTAS

Define los requisitos y casos en que se concede acceso remoto a las plataformas tecnológicas de la ALCALDÍA MUNICIPAL DE SOPÓ y las medidas de seguridad que se establece para la protección de la información que es accedida por este medio.

La política de conexiones remotas es extensiva para todos los funcionarios, contratistas y practicantes de la Alcaldía Municipal de Sopó que requieran y les sea autorizado el acceso a terminales o servidores institucionales a través de herramientas VPN para el desarrollo de sus actividades en horarios fuera de los normales o desde ubicaciones diferentes a las oficinas de la Alcaldía Municipal de Sopó.

6.8.1. Objetivos específicos para el uso de Conexiones Remotas

- Garantizar la confidencialidad, la privacidad y el uso adecuado y moderado de la información.
- Crear conciencia sobre los riegos asociados al acceso y gestión de información sobre las plataformas institucionales de manera remota y la manera de reducirlos aplicando los lineamientos aquí determinados.
- Especificar las recomendaciones y pautas necesarias para mantener segura la información y los elementos utilizados para el acceso y operación remota de información.
- Dictar las pautas para mantener organizado y resguardado las credenciales de acceso, así como los elementos de protección para asegurar la conexión remota.

6.8.2 Responsabilidades de la Oficina de Tecnologías de la Información y el Grupo de Soporte Tecnológico:

- Establecer e implementar los métodos de conexión remota a la plataforma tecnológica de la Alcaldía Municipal de Sopó
- Implementar los métodos y controles de seguridad para establecer conexiones remotas hacia la plataforma tecnológica Institucional.
- Restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.
- Verificar la efectividad de los controles aplicados sobre las conexiones remotas a los recursos de la plataforma tecnológica de la Alcaldía Municipal de Sopó de manera permanente.

DECRETO N°
(-- 135)

6.8.3 Responsabilidades de los usuarios:

- Contar con las aprobaciones requeridas para establecer dicha conexión a los dispositivos de la plataforma tecnológica de la Alcaldía Municipal de Sopó y deben acatar las condiciones de uso establecidas para dichas conexiones
- Mantener en total reserva las direcciones de entrada a las direcciones Institucionales (direcciones IP o direcciones Web) al igual que las credenciales que les han sido otorgadas para su resguardo.
- Mantener la confidencialidad y protección de la información a la que tienen acceso fuera de las instalaciones Institucionales.
- Aplicar herramientas de antivirus sobre sus computadores personales para brindar una mayor protección a los archivos e información que están gestionando.
- Dar aviso al Grupo de Soporte Tecnológico de cualquier posible abuso o intento de violación tanto de los accesos como de las credenciales entregadas.

6.8.4 Monitoreo:

- El área de Tecnologías de la Información en conjunto con la Secretaría de Desarrollo Institucional por medio del Grupo de Soporte Tecnológico, sin previo aviso, realizan brigadas de monitoreo para verificar el estado de las conexiones remotas y así generar el respectivo informe de lo encontrado.

Miguel Alejandro Rico Suárez
Alcalde Municipal

Segundo Hipólito Sanabria Alarcón
Secretario de Desarrollo Institucional

Diego Fabian León Beltrán
Profesional Universitario
Área de Sistemas de Información

Juan Carlos Rodríguez Camargo
Contratista Gobierno Digital